NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

UTILIZATION OF CONCURRENT BUFFERS TO FACILITATE SEAMLESS DATA TRANSITION IN TACTICAL CELLULAR COMMUNICATIONS

by

Darien M. Pitts

September 2015

Thesis Advisor: John Gibson
Second Reader: Gurminder Singh

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE UTILIZATION OF CONCURRENT BUFFERS TO FACILITATE SEAMLESS DATA TRANSITION IN TACTICAL CELLULAR COMMUNICATIONS		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Pitts, Darien M.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Applied Communications Sciences 150 Mount Airy Road Basking Ridge, NJ 07920		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The Department of Defense increasingly depends on secure, interoperable data networking. Emergence of devices leveraging media-independent handover technology, based on the IEEE 802.11 standard that was released in 1997 and addresses wireless local area networks. It also offers potential benefit to tactical networking. However, full implementation of IEEE 802.21-enabled networks for tactical use is currently infeasible due to design and deployment constraints.

This thesis serves to further research in the field of media independent handover, particularly with respect to enduring Transmission Control Protocol (TCP) sessions across heterogeneous media handovers. The principal purpose of the research is to introduce a top-level design for managing TCP sessions across the IEEE 802.21 handovers by instituting a set of synchronized TCP sockets across which an actual TCP session is tunneled. Included in the design is consideration for security of data at rest. To provide context, the tactical network environment is modeled using two current tactical simulations to demonstrate the degree to which tactical networks are subject to link discontinuities. The link discontinuities produce less than optimal communications in which an 802.21-enabled network may assist or mitigate.

14. SUBJECT TERMS IEEE, 802.21, Media Independent Handover, mobile, communications, cyber, tactical, buffer, cellular			**15. NUMBER OF PAGES** 91
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

UTILIZATION OF CONCURRENT BUFFERS TO FACILITATE SEAMLESS DATA TRANSITION IN TACTICAL CELLULAR COMMUNICATIONS

Darien M. Pitts
Major, United States Army
B.S., Tuskegee University, 2002
M.S., University of Maryland University College, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2015

Author: Darien M. Pitts

Approved by: John Gibson
Thesis Advisor

Gurminder Singh
Second Reader

Cynthia Irvine
Chair, Department of Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of Defense increasingly depends on secure, interoperable data networking. Emergence of devices leveraging media-independent handover technology, based on the IEEE 802.11 standard that was released in 1997 and addresses wireless local area networks. It also offers potential benefit to tactical networking. However, full implementation of IEEE 802.21-enabled networks for tactical use is currently infeasible due to design and deployment constraints.

This thesis serves to further research in the field of media independent handover, particularly with respect to enduring Transmission Control Protocol (TCP) sessions across heterogeneous media handovers. The principal purpose of the research is to introduce a top-level design for managing TCP sessions across the IEEE 802.21 handovers by instituting a set of synchronized TCP sockets across which an actual TCP session is tunneled. Included in the design is consideration for security of data at rest. To provide context, the tactical network environment is modeled using two current tactical simulations to demonstrate the degree to which tactical networks are subject to link discontinuities. The link discontinuities produce less than optimal communications in which an 802.21-enabled network may assist or mitigate.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
4G	4th Generation
ABCS	Army Battle Command System
ACS	Applied Communication Sciences
ADP	Automated Data Processing
AP	Access Point
ATCCS	Army Tactical Command and Control System
AuC	Authentication Center
BCT	Brigade Combat Team
BSC	Base Station Controller
BSS	Basic Service Set
BTS	Base Transceiver Station
CDMA	Collision Detection Multiple Access
CHAP	Challenge Handshake Authentication Protocol
COP	Common Operational Picture
COTS	Commercial-Off-The-Shelf
CPOF	Command Post of the Future
DHCP	Dynamic Host Configuration Protocol
DIT	Data In Transit
DOD	Department of Defense
DPD	Duplicate Packet Detection
DS	Distribution System
DTED	Digital Terrain Elevation Data
EIR	Equipment Identity Register
ENM	EPLRS Network Manager
ENP	EPLRS Network Plan
EPLRS	Enhanced Position Location Reporting System
FBCB2	Force XXI Battle Command Brigade
FBSS	Fast Base Station Switching
FHMUX	Frequency Hopping Multiplexer
GHz	Gateway Mobile Switching Center
GMSC	Gateway Mobile Switching Center
GPS	Global Positioning System

GRE	Generic Routing Encapsulation
GSM	Global Services for Mobile
HCLOS	High Capacity Line of Sight
HF	High Frequency
HLR	Home Location Register
HMMWV	High Mobility Multi-Purpose Wheeled Vehicle
HTG	Heterogeneous Tactical Gateway
IADS	Installation as a Docking Station
IDSS	Integrated Digital Soldier System
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv6	Internet Protocol, Version 6
ISR	Intelligence, Surveillance, and Reconnaissance
JBC-P	Joint Battle Command-Platform
JCSS	Joint Communication Simulation System
JNN	Joint Network Node
JNN-N	Joint Network Node-Network
L2	Layer 2 Networking
LCP	Link Control Protocol
LTE	Long Term Evolution
MACE	Multi-Access Cellular Extension
MAKP	Multi-Acces Key Planning
MDG	MACE Data Gateway
MDHO	Macro Diversity Handover
MFE	Multicast Forwarding Engine
MHz	Megahertz
MICS	Media Independent Command Services
MIES	Media Independent Event Services
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIIS	Media Independent Information Services
MOBIKE	Internet Key Exchange, Version 2 Mobility
MODEM	Modulator/Demodulator
MS	Mobile Station
MSC	Mobile Switching Center
MSE	Mobile Subscriber Equipment

NEC	Network Enterprise Center
NIC	Network Interface Card
NIE	Network Integration Evaluation
NSA	National Security Agency
NTC	National Training Center
OTAR	Over-The-Air Rekeying
P2P	Permanent Internet Protocol Address
PCD	Personal Communications Device
PIP	Permanent Internet Protocol Address
PPP	Point-To-Point Protocol
QoS	Quality of Service
RNC	Remote Network Controller
ROIP	Radio-Over-Internet Protocol
RS	Radio Set
SINCGARS	Single Channel Ground and Air Radio System
SMS	Short Message Service
SPEED	System Planning Engineering and Evaluation Device
SRTM	Shuttle Radar Topography Mission
STA	Station
STIG	Security Technical Information Guide
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
TIGR	Tactical Ground Reporting
TIP	Temporary Internet Protocol Address
TLS	Transport Layer Security
TTGS	Telcordia Technologies Government Solutions
UAS	Unmanned Aircraft Systems
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UE	User Equipment
UMB	Ultra Mobile Broadband
UMTS	Universal Mobile Telecommunications System
USCENTCOM	United States Central Command
UTRAN	UMTS Terrestrial Radio Access Network
VIP	Virtual Internet Protocol Address
VLR	Visitor Location Register

WiMax	Worldwide Interoperability for Microwave Access
WIN	Warrior Information Network
WIN-T	Warrior Information Network-Tactical

ACKNOWLEDGMENTS

I would like to acknowledge my advisors, John Gibson and Gurminder Singh, for their assistance throughout the process. Throughout the process, their assistance was invaluable. I would like to also thank Dr. Cynthia Irvine and Dr. Duane Davis of the Cyber Systems Operations curriculum at the Naval Postgraduate School, who devised a program exposing the students to a variety of subjects that stimulated ideas and fostered a productive learning environment. Also, I would like to thank all my instructors at the Naval Postgraduate School. Their teachings furthered my professional and technical development, which will prove instrumental in my military career.

I would like to thank some of my former military supervisors for entrusting me with managing some of the networks, technologies, and projects that I have worked with in the past. That knowledge was instrumental in thesis discovery and analysis. Working with some of the doctrine-changing initiatives, such as Installation As a Docking Station, and identifying some of the shortcomings of tactical communications experience on the battlefield was a driving force of this thesis.

Lastly, I would be remiss if I did not thank Jaewon Kang, Sunil Samtani, and Subir Das from Allied Communication Sciences for their expertise and information about the MACE project. Their assistance was pivotal in developing a viable and relevant thesis that may serve beneficial to the U.S. Army and Department of Defense.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OBJECTIVE

As mobile communications continue to become a dominant means of voice and data transmission, the desire to increase throughput and capabilities has increased as well. Over the past 10 years, the emergence of Bluetooth, 3G & 4G, WiMax, and other communication technologies has significantly changed the way we exchange data daily. Most current mobile devices are programmed to handle the changeover of networks of the same service (e.g., WiFi to WiFi). The IEEE 802.21 standard addresses the capability to provide continuous service while switching between different types of networks (e.g., WiFi to WiMax).

This thesis looks deeper into the IEEE 802.21 standard (IEEE, 2008). The standard addresses the capability for properly equipped devices, including cellphones and tablets, to access the data transmission services, whether homogeneous or heterogeneous, within their area of operation and switch to the optimum service. It is predicated on meeting certain prescribed conditions and allowances. In tactical situations, units and personnel move on the battlefield and thus need robust network changeover capabilities, more commonly referred to as hand-overs or hand-offs. Uninterrupted updates to maps and the sharing of streaming intelligence data are both applications that would benefit from improved changeover technology.

Through research, analysis, and simulation, the objective of this thesis is to delve into known issues with the IEEE 802.21 standard and find ways to mitigate them, allowing for wider acceptance and usage. The main contribution of this thesis is a proposed architecture for incorporating synchronized data buffers into 802.21-enabled end-user devices in order assist in the handover process between multiple mobile data services. Additionally, we assess the standard's use in military and tactical environments for future use in supporting the communication needs and mission objectives for units that may one day utilize the technology.

B. WHAT IS 802.21?

Manufacturers of mobile devices, including smartphones and laptops, have been including multiple network interfaces in their designs to utilize current communication technologies. Taniuchi et al. (2009) assert that "as the trend in multi-interface devices continues, operators with multiple networks must facilitate easy access across their multiple technologies through a single device. Supporting seamless roaming and inter-technology handover is a key element to help operators manage and thrive from this heterogeneity" (p. 112).

IEEE 802.21 is an emerging standard intended to address the problems currently associated with facilitating multiple interfaces in mobile telecommunication devices. It does so "by providing a media-independent framework and associated services to enable seamless handover between heterogeneous access technologies" (Taniuchi et al., 2009, p. 112). Referred to as media-independent-handover (MIH), the technology uses protocols programmed within a device and servers (or other equipment) to enable network nodes to constantly seek media access technologies that allow optimum and reliable data transmission with few to no disconnections or other issues during switching.

The principal components that compose IEEE 802.21 standard are discussed in greater detail in Chapter II, as well as issues associated with service handovers that prevent wide acceptance of the standard in both commercial and military devices.

C. RELEVANCE

1. Relevance to Cyber Operations

The word cyber is derived from the Greek word *kybernetes* and is defined as "of, relating to, or characteristic of the culture of computers, information technology, and virtual reality" (Cyber, n.d.).

The individual components of all that is deemed under the realm of cyber operations incorporate ever-changing technologies and governance. Along with the changing technologies, issues such as security, greater bandwidths and faster transmission rates, and compatibility will continue to push the revolution.

This thesis addresses the IEEE 802.21 standard and relevant security issues, including protection of buffered data-and the need to use encryption to protect that data, as well as the integration of existing telecommunication technologies, such as Transport Control Protocol (TCP), a reliable data transfer protocol, to ensure consistency of data exchanges. Results from previous and current cyber initiatives involving 802.21 are investigated and incorporated, with the intention of making relevant and concise contributions to the advancement of the standard.

Mobility is a significant part of cyber operations and the Department of Defense continues to operate in changing and challenging environments. Operating within these environments has led to considerations regarding the adoption of 802.21-enabled devices as a viable means of mobile communications. Mobility in a heterogeneous networking environment may require switching between multiple types of networks. As IEEE 802.21 supports the requirement, it is possible that its capabilities may one day be commonplace in all smartphones, tablets, etc. This research addresses issues pertinent to IEEE 802.21 and suggests measures for future research and use.

2. Relevance to the Army and DOD Operations

Extensive developments have been undertaken to keep our military forces and Department of Defense (DOD) agencies on the cutting edge of mobile technology to give operational advantage to the United States over adversary states. Significant examples include the Mobility Capability Package initiatives of the National Security Agency (NSA), the Future Warrior Program of the United States Army, and future increments of the Warrior Information Network-Tactical (WIN-T) program, which is also part of the United States Army's communication infrastructure.

In the area of tactical operations, decision makers aspire to acquire a better and sharable common operational picture (COP), allowing commanders at all echelons to make better, more accurate decisions in real-time. Simultaneously, shrinking budgets and economic fluctuations potentially hamper the adoption of some of the aforementioned technological advances, despite the fact that aging technologies rapidly lose their relevance, utility, and widespread usage. Also, known issues and challenges such as

limited availability of frequencies in the radio frequency spectrum and the pending switch to the IPv6 addressing scheme result in demand for technologies able to operate within the constraints and availability of current and emerging communications media.

This research has the potential to benefit multiple agencies within the Department of Defense, especially the Army and the Marine Corps, during tactical deployments. IEEE 802.21 devices may contribute to ensuring that data are securely available on the battlefield. This research can also be applicable to other DOD agencies, as ad-hoc network solutions may be deployed during crises. IEEE 802.21-enabled devices can provide a stable, alternate capability for data connectivity and additional means of communication in situations experiencing both tactical equipment and frequency shortages. Another benefit of this thesis is that it can provide DOD agencies the capability to utilize their own independent tactical data networking for mobile operations, eliminating the need to modify all mobile equipment and infrastructures in times of deployment.

D. RESEARCH QUESTIONS

The following research questions are addressed through in-depth research and simulation experimentation:

- What is a feasible technique, within the existing software and hardware infrastructure, to assist in seamless service handover? How might data integrity and device authenticity be maintained as the device migrates across underlying communications systems?
- What type of strategic and flexible tactical deployment strategy for communication nodes utilizing the 802.21 standard will ease Media Independent Handover (MIH) service handovers in tactical environments compared to the stationary nodes utilized in commercial environments?

II. BACKGROUND

A. IEEE 802.21

1. Introduction

In recent years, the demand for mobile technologies capable of using multiple broadband data solutions, such as wireless local area networking (WiFi), Worldwide Interoperability for Microwave Access (WiMAX), and 3G/4G cellular, has grown rapidly. Along with the demand has come a need to create "handover solutions that can seamlessly and securely transition user sessions across different access technologies" (Taniuchi et al., 2009, p. 112). There have been challenges along the way, for each step toward seamlessly addressing issues such as latency, data loss, and security guarantees. The IEEE Standard 802.21 addresses this set of problems and also suggests policies to govern the handover solutions (Taniuchi et al., 2009). This thesis investigates options for utilizing the technology for tactical use.

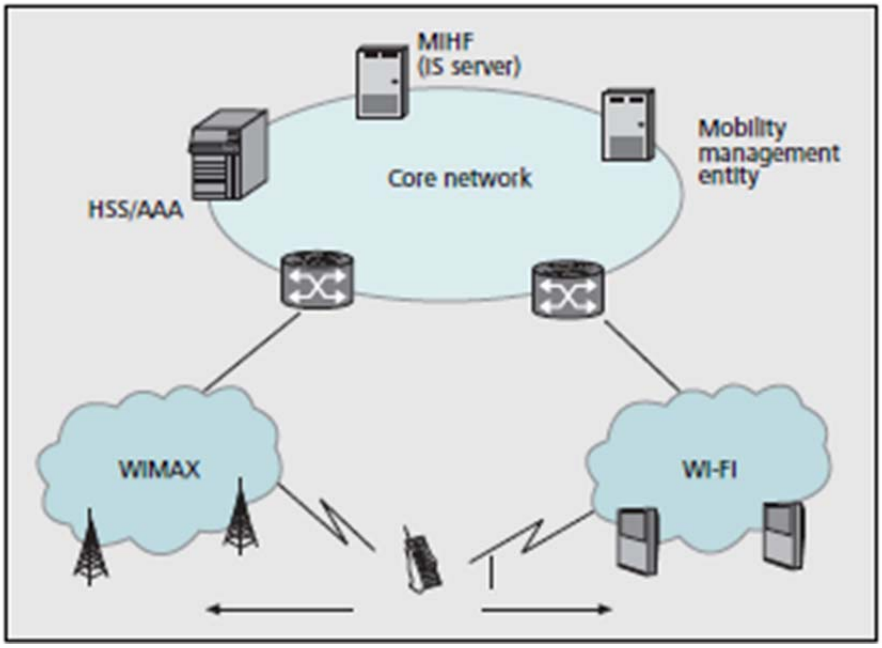

Figure 1. General Concept of Service Handover in 802.21 (from Taniuchi et al., 2009)

The IEEE 802.21 standard is composed of multiple components that manage the complex function of facilitating a transfer of application sessions between network services. When executing a transfer of services, referred to as MIH, the transfer may be between different networks within the same service (e.g., two different WiFi services) or two entirely different services (e.g., WiFi to WiMax), as seen in Figure 1. Through an intricate process of evaluating available services and choosing the optimum of those, the standard prescribes a methodology to provide seamless data connectivity (Pinho, 2008). Figure 2 shows a basic and undetailed look at how MIH works to connect data access services. It serves as a shim between the local access layer (Data Link Layer, not limited to IEEE 802 family of protocols) and the internetworking (Network, typically IP) layer. Some of the major components that allow the 802.21-enabled devices to operate are discussed further in this thesis.

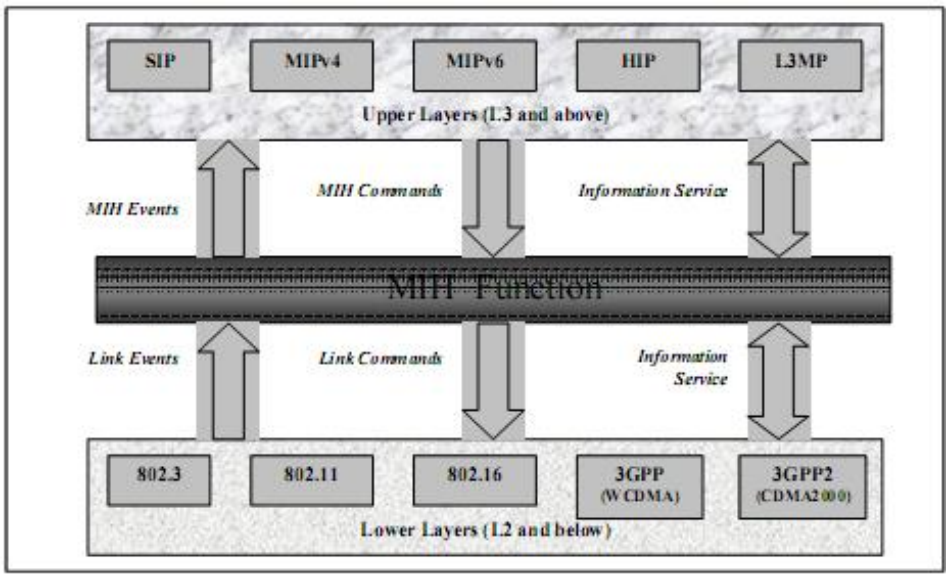

Figure 2. MIH Component Interactions (from Pinho, 2008)

The Media Independent Handover Function (MIHF) is one of the principal components that "provide[s] events, controls and even information for an application to use" (Dutta et al., p. 3). This component is also the core of the 802.21 operation mode and provides three main services: Media Independent Event Services (MIES), Media

Independent Information Services (MIIS), and Media Independent Command Services (MICS), as depicted in Figure 3 (Pinho, 2008).

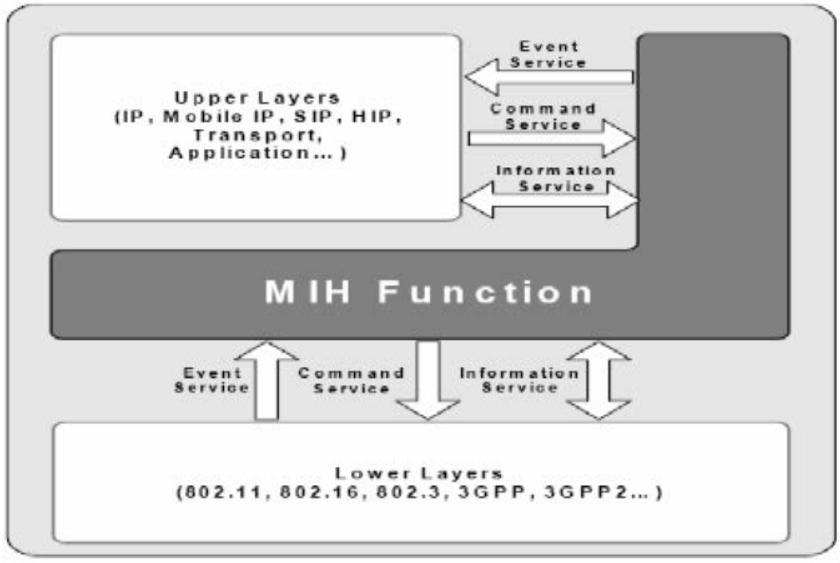

Figure 3. MIHF Location in 802.21 and Key Services (from Dutta et al., p.3)

The Media Independent Event Service is "responsible for detecting events and delivering triggers from local and remote interfaces" (Pinho, 2008, p. 20). Local events are defined as those that occur within the client device, while remote events occur within the network external to the device. Some of the events that occur include: Link Down, Link Up, L2 handover Imminent (as in layer 2 networking), and Link Parameters Change. Figures 2 and 3 show the Media Independent Handover Function, as well as what is considered upper and lower-level access services. The governing application on a client device usually resides in the upper layer services (as shown in the figures), but it may get notifications from the lower layer services as events take place (Dutta et al.).

The Media Independent Information Service "provides the information model for query and response, [and] make[s] the handover decisions more effective" (Pinho, 2008, p. 20). Since mobile 802.21-enabled devices are designed to discover neighboring networks and communicate with portions of these networks in order to facilitate and optimize handovers, the MIIS defines the information producing elements and the "query-response mechanisms that allow an MIHF entity to discover and obtain

information relating to nearby networks" (Dutta et al., p. 3). The information may be either dynamic or static and include data such as names and providers of neighboring networks, channel information, pertinent security information, MAC addresses, and other information deemed relevant to handovers (Dutta et al.).

The Media Independent Command Service "provides a set of commands for the MIHF users to control handover link states" (Pinho, 2008, p. 20). These commands may be local and remote and may come from the upper layer services to the MIH, as well as from the MIH to the lower layer services. Basically, the commands govern how a MIH device polls connected links to learn of status, learn of discovered links, switch between available links, and to configure new links (Dutta et al.).

2. Current Status

There are several cell phones and notebook computers on the market that support mobile data access technologies such as IEEE 802.11 (WiFi), 3G cellular, 4G cellular, and LTE (long-term evolution). As manufacturer requirements and customer expectations grow, the development of multi-interface mobile devices will continue. A bi-product of the development, the need for "supporting seamless roaming and inter-technology handover is a key element to help operators manage and thrive" (Taniuchi et al., 2009, p.112).

Though 802.21 implementation does not dominate cellular and computing markets yet, there are efforts by the working groups for the IEEE standards 802.16 (WiMax) and 802.11 (WiFi) to modify aspects of their standards for increased interoperability with future 802.21-enabled devices. The amendments to the parameters of homogeneous-natured technologies will make them more adaptable to heterogeneous handovers (Taniuchi et al., 2009).

3. Multi-Access Cellular Extension (MACE)

Though 802.21 networks may vary as the technology is developed, this thesis examines the work of Applied Communication Sciences (ACS) along with Telcordia Technologies Government Solutions (TTGS). Under contract to the U.S. Army, these

companies developed the MACE program, and remain the key developers as it progresses.

The purpose of the project is to develop stable 802.21 networks and devices for tactical and military use. The network includes components of widely used data access technologies (WiFi, 3G/4G, etc.) and COTS Android-based phones and tablets. The information that is available about the project's efforts, issues, and achievements served as the primary motivation and resource for thesis.

A typical MACE topology may consist of multiple base stations and end-user devices with components that govern or assist in service handovers. These base stations have antennas, servers, and applications that facilitate handovers and track information about surrounding network infrastructures that may be utilized in its topology (i.e., nearby WiFi connections). The end-user devices interact with 802.21 network components as well as those from other service providers for data access and handover assessment functions.

In addition to the services and components of typical 802.21 implementations discussed in the previous section, MACE networking introduces various other components, both in software and hardware, which assist handover decision making and performance enhancement, particularly for tactical employments. The Heterogeneous Tactical Gateway (HTG) is an IP-based software application "that provides seamless handoff across all available networks, mesh networking, multicast, and key security features" (Applied Communication Sciences, 2012, p. 2). Several HTG entities can be centralized or distributed with settings instituted for redundancy and resiliency. Each forwards unicast and multicast data among the end user devices that are part of the same domain (Applied Communication Sciences, 2012).

The MACE network includes a MACE Data Gateway (MDG) and enabled end-user devices one hop away from the MDG. The network includes security measures for Data In Transit (DIT) at the link, network, and transport layers of networking. MACE utilizes Generic Routing Encapsulation (GRE), which is a tunneling protocol used to encapsulate data and other network protocols to facilitate point-to-point Internet Protocol

connections, between the MDG and each device in its domain in order to send unicast and multicast traffic to other devices in the same domain. For inter-domain communication, Internet Key Exchange, version 2 (IKEv2) Mobility, known as MOBIKE, is used with GRE to ensure the tunnel is not reconfigured when addressing service connectivity changes in an end-user device (Applied Communication Sciences, 2012).

The MDG has multiple software components that administer the tasks allowing it to conduct inter-domain communication. A key component of MDG is the Multicast Forwarder controlled by the Multicast Forwarding Engine (MFE) that "performs the actual socket operations of reading the data, checking the cache for forwarding decisions, checking the DPD [Duplicate Packet Detection Cache] for prior existence of the packet and then performing the actual transmission on each of the target interfaces" (Applied Communication Sciences, 2012, p. 27).

Other components in the MACE architecture have critical roles, including the multicast forwarder that enables multicast over tactical cellular infrastructure. It "creates and maintains a dynamic vendor and radio access technology agnostic overlay to enable native multicast packets to traverse the cellular network to and from [the] smart devices" (Applied Communication Sciences, 2012, p. 4). The Multi-Access Key Planning (MAKP) server is part of the MACE architecture that can be hosted on the HTG or on a separate server. It interfaces with the Internet Protocol Security (IPSec) or Transport Layer Security (TLS) modules on end-user devices providing the keys and necessary credential information.

4. Benefits

The IEEE 802.21 standard provides multiple benefits for device users and network operators. As mentioned earlier, it allows users (and their enabled devices) to elect among several different types of networks: WiFi, WiMax, and 3rd Generation Partnership Project (3GPP/3GPP2[1]) networks, which include LTE (Long Term

[1] 3GPP2 is a separate initiative from 3GPP that includes the defunct Ultra Mobile Broadband (UMB) project, as well as several of the CDMA2000 cellular technologies.

Evolution) as well as UMTS (Universal Mobile Telecommunications System). Mobile subscribers can be notified when networks become available and handovers occur; events can also be monitored and reported to the 802.21-enabled devices. The handovers can be configured based on selected preferences and organization policies (Jain, 2010).

There are multiple benefits seen in the key functions of 802.21. Reduced power consumption on enabled mobile devices is beneficial for long-term use during device employment and operation. This is done by avoiding unnecessary scanning and enabling of service modules, like WiMax, within a device only if the respective service is available and desired. Also, power consumption on a device is reduced by using the core network to do some of the decision making. Service providers can independently enforce their policies and other agreements, which is also an ideal attribute for tactical networking, assuming the tactical organization controls the core network.

Reduced handover time is another benefit that may come from 802.21 key functions. Compared to handovers in homogeneous networks, handover time in 802.21 networks is reduced as the security and quality of service (QoS) requirements are passed to neighboring nodes (Jain, 2010). Furthermore, the interoperability domain is simplified in that "a media-independent framework is a more scalable and efficient method of addressing inter-technology handovers. With a common platform in place to address handovers, each access technology requires only a single extension to ensure interoperability with all other access technologies" (Taniuchi et al., 2009, p. 113).

5. Issues

The major impediment to the widespread use of 802.21 services is the inability to guarantee seamless handover functions without data loss. Imagine a user watching a streaming video or an Army Division commander watching an 802.21-enabled device to monitor a constantly changing map as units move around on the battlefield. If there was a service handover between heterogeneous networks, there is no guarantee against the loss of data packets during the transition (Applied Communication Sciences, 2012). In discussing handovers in a non-optimized environment, Dutta et al. remarked, "In the case of non-optimized handoff scenario (without 802.21 and MPA mechanisms), the handover

delay and packet loss take place during the mobile's movement, IP address assignment, post-authentication, and mobility binding update. The DHCP interaction takes a long time to complete the detection of duplicate IP addresses and the binding updates can be delayed if the correspondent node is too far from the mobile node" (Dutta et al., 2012, p. 6). It should be noted that homogeneous network handovers (e.g., WiFi to WiFi) typically do not experience as many handover failures as experienced by heterogeneous networks (e.g., WiFi to LTE).

Another challenge is to find a feasible and efficient solution that meets all outward requirements while ensuring seamless handovers. Ensuring security, whether during session handover or with data-at-rest, has always been an aspect of great concern in most of the implementations of IEEE 802.21 networks and technology developed over the years (Buiati F. , Saadat, Canas, & Villalba, 2011). Encryption schemes, which will be explained in greater detail later, have evolved in the effort to reduce latency issues while providing proper communications security.

Other issues include addressing scalability, interoperability, and network complexity.. Dutta et al. states "an important challenge facing IEEE 802.21 is the unification of all the media-specific technologies under one abstract interface" (p. 6). The source goes on to stipulate "this approach may be difficult to realize in practice within a short period of time due to the large number of technology-specific standards within and outside the IEEE 802 systems that must be extended to conform" (p. 6).

Adding to the issues of successful handovers in 802.21 networks is the fact that most end-user devices are constantly in motion therefore calling for constant searching for available networks and assessing accessibility. The constant probing adds to depletion of device battery life and non-optimized network environments. IP address assignment, encryption, and authentication all depend on accurate and concise assessments; each requires expenditure of device power resources.

Scalability and interoperability become problematic within wireless networks as access issues such as hidden node and exposed node problems may occur. In a hidden node scenario, "basically client devices that are all within range of the WLAN access

point (AP) but are not necessarily within range of each other" (Wexler, 2007). An exposed node problem "occurs when a node is prevented from sending packets to other nodes due to a neighboring transmitter" (Kapadia, Patel, & Jhaveri, 2010). These two access issues are usually problematic in homogeneous networks, but may become cumbersome as handover decisions are done by MIHF for both homogeneous and heterogeneous services (Taniuchi et al., 2009). Procedures regarding security and device functionality may differ among commercial corporations (service-providers and device-manufacturers) and may lead to additional concerns (Dutta et al.).

In terms of interoperability and overall success of implementation, additional primitives and extensions may need to be added to the participating access services, such as 802.11 and 802.16, in order to support MIH services. Dependence on individual service providers and device manufacturers willing to comply and adopt their current or future devices, protocols, etc., without regard to market objectivity is also key to the widespread use of 802.21, both commercially and tactically. Implementations that disregard adding the necessary extensions may result in operational issues, such as degraded device battery life and inconsistent interoperability.

B. OVERVIEW OF MOBILE COMMUNICATIONS

In this section, we briefly describe three common mobile communication infrastructures. Each of the respective infrastructures is set up with some form of base stations, external access points, and supports interoperability with a multitude of end-user devices. They are prime candidates for participation in 802.21-enabled internetworking.

1. IEEE 802.11 (WiFi)

Variations of the IEEE standard 802.11, better known as WiFi, is the preferred standard of wireless data access around the world (Pinho, 2008). The family of standards "define(s) a through-the-air interface between a wireless client and a base station access point or between two or more wireless clients" (AIR802, n.d.).

The infrastructure of a typical 802.11 network consists of an access point (AP), depicted in Figure 4, by which any WiFi-enabled device, called STA (station), within the

AP radio range may access the local area network. This network connection may be extended through the AP to the Internet through a service provider MODEM or broadband connection in the host facility, as well as a mobile phone that incorporates the access point as an embedded mobile hotspot. The STA may be either mobile or fixed, as may also be the case with the AP. If either the AP or its STA is mobile, it may need to participate in a handover process. The Basic Service Set (BSS) comprises the coverage area for STAs to connect to access points. A Distribution System (DS) may interconnect access points forming a much larger access network footprint. In this case, there is an Extended Service Set (ESS) that comprises a complex grouping of DS and BSS entities. There is an established portal that connects 802.11 networks with different networks providing internetworking services (Pinho, 2008). Figure 4 illustrates the various WiFi components and how they interact.

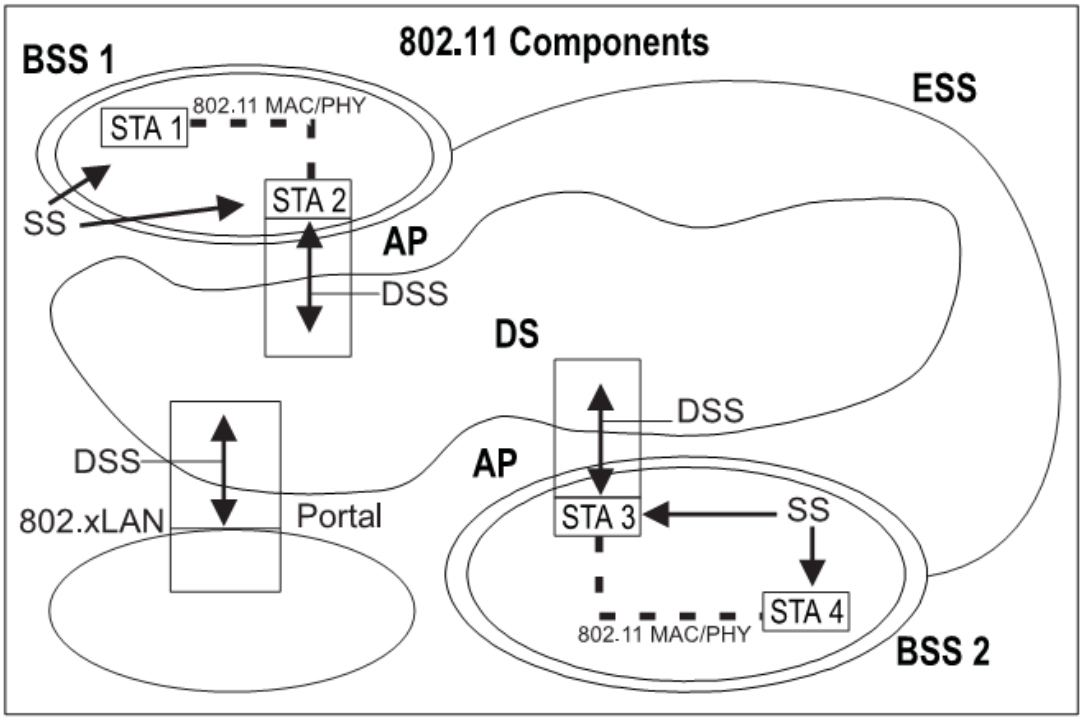

Figure 4. Diagram of a Typical 802.11 (WiFi) Network (from Pinho, 2008)

As a station detects an AP, the decision processes needed to connect or disconnect are executed. There is an authentication process followed by an association process

before any data frames are transmitted. There are three stages, or states, in which each of the authentication and association processes are involved. The stages bifurcate to accomplish authentication as well as association. The same occurs for termination of the authentication and association states.

For an 802.11 network to conduct a handover, the connection to a new station or AP starts with a scanning phase for discovery. Upon discovery of a suitable station or AP, there is a switching phase. This is followed by the authentication and association phases with the newly found entity (Pinho, 2008).

There are different types of 802.11 devices available related to the specifications of the standard variant by which they abide. Some devices are capable of employing multiple variants. Those usually seen in most WiFi devices are 802.11a, 802.11b, 802.11g, and 802.11n, with 802.11ac emerging. Each is defined by parameters such as frequency bands, number of scanning channels, throughput, etc. Many of the wireless router products sold in retail markets today utilize the 802.11n specification because it is capable of operating in the same frequency bands as both 802.11a and 802.11b. For the most part, small-business owners and consumers that use routers at their facilities are compelled to buy the 802.11n devices since they are the latest to be broadly sold, without the consumer fully understanding of the implementation attribute. Although the 802.11ac variant is emerging and offers greater throughput and range than previous variants (AIR802, n.d.).

Table 1 compares the characteristics of the WiFi specifications available commercially (802.11ac was still a draft standard as of November 2013 with final IEEE Standards Board Approval projected for Feb 2014) (Mccann & Ashley, 2014).

Comparison of 802.11 LAN Standards				
Standard	**Maximum Data Rate(Mbps)**	**Typical Throughput (Mbps)**	**Operating Frequency Band**	**Maximum Non-Overlapping Channels (Americas)**
802.11b	11	6.5	2.4 GHz	3 *1
802.11g	54	8 (Mixed b/g) 25 (Only 802.11g)	2.4 GHz	3 *1
802.11a	54	25	5 GHz	24 (20 MHz channels) 12 (40 MHz channels)
802.11n	600 (Theoretical Max)	74 to 144 *2	2.4 GHz & 5 GHz	*3

*1 - Channels 1, 6 and 11 are the three non-overlapping channels in the Americas. Each channel is 20 MHz wide.

*2 - These are typical achieved rates. Actual throughput will depend upon various factors such as the manufacturer and model, environmental factors, whether 20 MHz or 40 MHz channels are utilized, if security is enabled and whether all clients are 802.11n or a mix of 802.11a/g/n.

*3 - For 802.11n, in the 2.4 GHz band, there are three non-overlapping 20 MHz channels or one 40 MHz channel. The use of 40 MHz is not desirable or practical in the 2.4 GHz band. However, a single 20 MHz channel could be used with lower throughput, largely defeating the gain of using 802.11n. In the 5 GHz band, twenty four non-overlapping 20 MHz or up to twelve 40 MHz channels exist.

Table 1. 802.11 LAN Standards (after AIR802, n.d.)

2. IEEE 802.16 (WiMax)

The IEEE 802.16 (Worldwide Interoperability for Microwave Access) family of standards (and succeeding amendments) encompasses broadband wireless access. Unlike infrastructure-based WiFi, which is essentially a point-to-multipoint architecture, this data service employs a point-to-point architecture with multiple types of topologies. In each configuration of operation there is a central base station (BS), multiple subscriber stations (SS), and antennas by which devices communicate (Pinho, 2008).

Pertinent to the subject of this thesis, is the fact that the IEEE standard 802.16e is an amendment that prescribes WiMax for mobile operations. This amendment to the standard discusses three optional handover operations that may not actually be implemented in typical 802.16 networks. The optional operation methods are base

operation method, Macro Diversity Handover (MDHO), and Fast Base Station Switching (FBSS). Table 2 shows the foundational principles of how MDHO and FBSS handover operations occur. Similarities between handovers in 802.16 and 802.21 can be seen, though 802.16 implementations apply to homogeneous networks, i.e., 802.16, whereas 802.21 implementations apply to heterogeneous networks (Pinho, 2008).

Handover Decisions in 802.16e

1. Handover Decision. In MDHO, the step begins with the decision to transmit and receive from multiple BS at the same time. In FBSS, the handover is started with the decision to receive and transmit data to an Anchor BS.
2. Diversity Set Selection/Update, where the mobile node scans the neighbor BS and select the ones to include in the diversity set.
3. Anchor BS Selection/Update, whereas the mobile node monitors the signal strength of the BS in the Diversity Set, and selects one BS to be the Anchor BS.

Table 2. 802.16e Handover Decision Stages (after Pinho, 2008)

There are several interesting features of WiMax that make it an ideal candidate for study. It is known to have lower power consumption for mobile stations than other data transmission technologies, as well as a sleep mode, while still allowing for service handovers. Mobile WiMax also utilizes smart antenna technologies that allow better coverage and performance. Other features include an operating frequency of 2500 MHz with multiple and scalable channel bandwidths available (Kivisto & Jarvela, 2006).

3. Universal Mobile Telecommunication System

The Universal Mobile Telecommunications System (UMTS) is the standard that governs 3rd Generation (3G) migration of Global Services for Mobile (GSM) networks. It defines packet-based transmission of digital voice, short message service (SMS), and other data (like streaming and multimedia) (Rouse, 2006). It builds on the improvements of 2nd Generation (2G) networks, including features such as wider bandwidth, Internet access, and quality of service parameters (Pinho, 2008). Like GSM, resources are

allocated to individual subscribers for the duration of their communications session. Specifically, voice sessions remain circuit-switched, while data sessions comprised of data packets are transferred from the cellular network to a packet-switched network by the cellular infrastructure.

Figure 5 shows a typical UMTS network and its various components. It consists of the following components: User Equipment (UE) or Mobile Station (MS), such as handsets or UMTS-capable remote sensor nodes; a Base Transceiver Station (BTS), referred to as a Node B in UMTS; a Base Station Controller (BSC), referred to as a remote network controller (RNC); a Mobile Switching Center (MSC); and a core network comprised of a Visitor Location Register (VLR), a Home Location Register (HLR), an Authentication Center (AuC), a Gateway MSC (GMSC), and an Equipment Identity Register (EIR) (Pinho, 2008). A BTS includes the radio equipment used to make the physical layer (wireless) connections, whereas the BSC controls and manages a set of one or more stations (BTS). A MSC provides connection to other MSCs and BSCs, and the GMSC provides access to the public telephone network. The VLR and HLR both store UE/MS location information; however, the first only stores information pertinent to UE/MS equipment temporarily residing on the host network due to their mobility. The HLR stores information for all users subscribed to the hosting network provider. The AuC contains the algorithms for authenticating subscribers, as well as keys for encryption. The EIR stores identities of all the Mobile Stations allowed access to the network, tracking them by their International Mobile Equipment Identity (IMEI) (Rouse, 2006).

Some of these components are comparable to the major components in an 802.21 (MIH) network. The premise underlying the functionality of a UMTS network is comparable to an 802.21 network in that both are intended to maintain continuous data connectivity once a link has been established and the user equipment is in transit (effectively mimicking circuit switching). The difference is that the user equipment in UMTS moves among homogeneous networks compared to heterogeneous networks utilized with 802.21-enabled equipment (Rouse, 2006). Figure 5 includes UMTS functionality and the subsystem necessary for backward compatibility to GSM (i.e., 2nd

generation—GSM BSS). Thus, the GSM BTS and BSC nodes form the radio access network for the GSM functionality. The UMTS Terrestrial Radio Access Network (UTRAN) is comprised of the RNC and Node B devices and forms the radio access network for the 3rd generation system (Rouse, 2006).

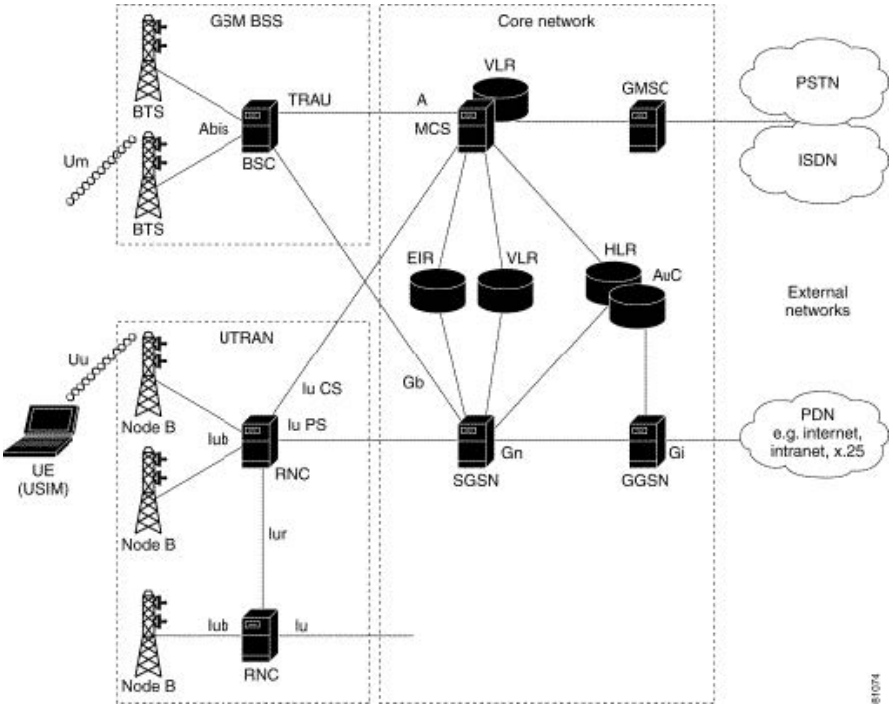

Figure 5. Diagram of UMTS Network (from Pinho, 2008)

C. OVERVIEW OF MILITARY COMMUNICATIONS

1. Mobile Subscriber Equipment

In the 1970s, tactical Automated Data Processing (ADP) systems deployed and provided the backbone of modern U.S. Army communications, and they were designed to give American soldiers capabilities that no other army possessed at the time. By definition, ADP systems were intended to remove some of the human decision in processing data. As these ADP systems evolved, they developed into what is currently called the Army Battle Command Systems (ABCS) (Defense Department, Army, Fort Monmouth Historical Office, 2008).

As the use of the ABCS increased and technology advances occurred in both private industry and the military, more dependable and deployable communication assets became necessary. Reliability, security, and more bandwidth were growing concerns as well. As Army systems further adopted the technological advances seen in several civilian industries, force modernization continued and the term, Force Modernization, described the efforts leading into the eighties (Defense Department, Army, Fort Monmouth Historical Office, 2008). Force modernization led to the development of multiple systems still used today by the Army and the Department of Defense.

Other than the Single Channel Ground and Air Radio System (SINCGARS), the development of the Mobile Subscriber Equipment (MSE) became one of the largest advancements in Army and Joint communications. The premise of MSE was that soldiers should be able to communicate effectively anywhere on the battlefield, whether deployed forward or stationed at a command and control node. SINCGARS, various high frequency (HF) radios, voice and packet switching technologies, and various COTS systems comprised the makeup of MSE. The equipment was placed in different shelter configurations designed to support voice and data services. The configuration, as shown in Figure 6, suited the Army doctrine of combat operations at the time (Global Security, Mobile Subscriber Equipment (MSE), 2011).

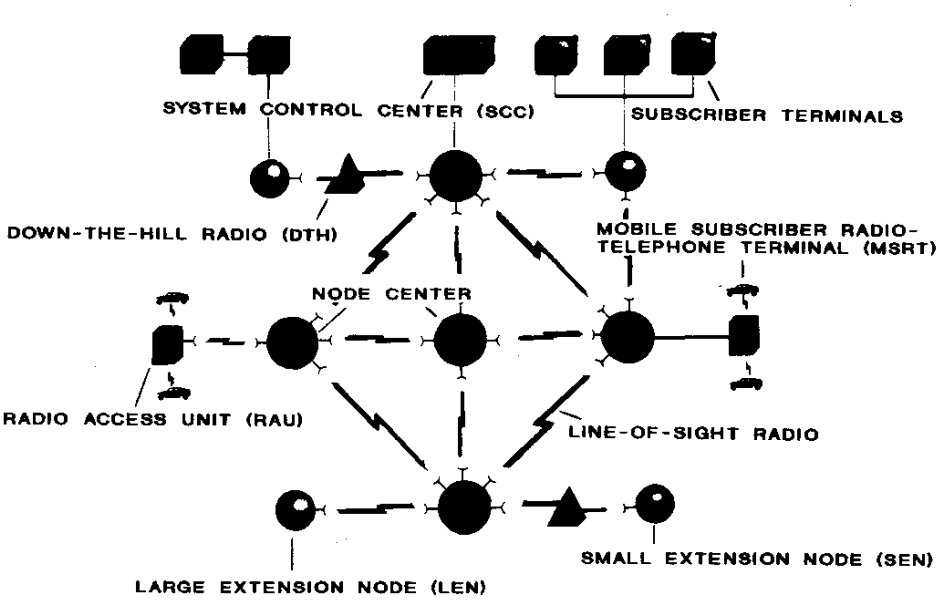

Figure 6. Mobile Subscriber Equipment (MSE) Assemblages and Technology (from Global Security, Mobile Subscriber Equipment (MSE), 2011)

As MSE went through several iterations of improvement, the ABCS increased in sophistication with more graphics processing and bandwidth capabilities. Among these ABCS systems, the most resource intensive collaborative tool was the Command Post of the Future (CPOF). Its arrival around the end of the century monopolized the data capabilities of the MSE assemblages and further pushed more capabilities than the outdated equipment could provide. Streaming video and teleconferencing started to play more of a part in providing leaders with the common operational picture (COP) needed for quick, decisive actions. The limited throughput and changing style of approaching combat and unit alignments called for even more mobile and robust means of communication, along with more availability of bandwidth and increasing means of network security (Global Security, Mobile Subscriber Equipment (MSE), 2011).

In 2004, United States Central Command (USCENTCOM) presented an urgent needs statement calling for greater capabilities than provided by MSE, as expenses

mounted for what was deemed antiquated equipment. There was already a long-term initiative in the plans at the time called the Warfighter Information Network (WIN). The Joint Network Node (JNN) was quickly conceptualized as a more cost effective and short-term solution to the WIN initiative (Global Security, Mobile Subscriber Equipment (MSE), 2011).

The changeover from an MSE-dominated armed force to one integrating the new and improved Joint Network Node approach to tactical communications would prove to be a major undertaking. JNN built considerably upon the concepts of MSE, with strategies to adapt to upcoming technologies and best business practices of the time as well as in the future. Most of the MSE assemblages and separate equipment began to be phased out of the Army's inventory around 2004. Though the majority of the assemblages were becoming obsolete, some had ongoing purposes that would warrant their continuance. Of the legacy systems, the High Capacity Line of Site (HCLOS) radio and its supporting subcomponents, the Frequency Hopping Multiplexer (FHMUX) radio, and Band I and III antennae are still used to a limited extent today (Global Security, Mobile Subscriber Equipment (MSE), 2011).

2. Enhanced Position Location Reporting System (EPLRS)

Some of the functionality of the Enhanced Position Location Reporting System makes it a candidate for modeling and simulating IEEE 802.21 concepts. The information below provides an overall description of the technology as well as the functions that pertain to the modeling to be described later.

EPLRS was first fielded in the United States Army's inventory in 1987 as a solution to support one of the functional areas of the Army Tactical Command and Control System (ATCCS). The system helped the accuracy of battle management and planning because of its ability to supply real-time positioning data of both friendly and enemy forces. The first systems were quite large and only meant to be located at tactical command centers. Efforts to make the systems more compact continued and, in 1991, smaller command post models were available, as well as ones for High Mobility Multi-purpose Wheeled Vehicles (HMMWVs). The EPLRS has become the engine behind the

multifunctional Force XXI Battle Command Brigade and Below (FBCB2) system (Federation of American Scientists, 1998).

The EPLRS consists of much more than just radios. “EPLRS is a network of wireless tactical radios that distributes digital data from many mobile users to many other mobile users. The EPLRS network consists of many EPLRS radio sets (RSs) and one or more EPLRS Network Manager (ENM) host computers” (Fielke, 2007, p. 1). The components of an EPLRS network include host computers, and supporting equipment (antennas, harnesses, wiring, etc.). Figure 7 shows a vehicular mountable EPLRS radio that is typically used in HMMWVs and a Micro-Light EPLRS that may be used in unmanned aerial vehicles (UAVs).

Figure 7. Vehicular and Micro-Light EPLRS with Computer (from Fielke)

The functions of the EPLRS radio and network make it an attractive for a case study. “The EPLRS network is a reliable system that automatically reconfigures itself to overcome the line-of-sight limitations of UHF communications as well as jamming threats” (Raytheon Company, 2014, p. 4). It uses a Time Division Multiple Access (TDMA)

structure. “Each RS [radio set] in a community is assigned slices of time (called timeslots) in which the RS can transmit while other RSs can receive. To accomplish this, each RS possesses a clock that is synchronized to the clock of every other radio” (Tharp & Wallace, p. 207).

There are other relevant functions of the EPLRS radio and network. It has four levels of relay that allow reconfiguration including low and high data rate modes. It is capable of using GPS data as an input, but it is not necessary for giving location data to other nodes in the network. This is helpful when jamming is a possibility. In terms of security, EPLRS radios are capable of performing over-the-air-rekeying (OTAR) in order to distribute keys to other nodes or from a governing system. Other features include messaging capabilities, embedded error correction, and multiple operating modes (Tharp & Wallace).

The most important function that makes it an ideal candidate for modeling an 802.21 network is the fact that EPLRS networks are self-healing. “If a selected networked communication path is unexpectedly interrupted, EPLRS will automatically seek alternative routing, eliminating the necessity of manual intervention by a communication network controller” (Tharp & Wallace, p. 207). This is accomplished through the creation of virtual circuits, called needlines, which are generated in both point-to-point or broadcast communications by transmitting one of four different types of needlines to get updates. The four different types of needlines are: Carrier-Sense Multiple Access (CSMA), Multi-Source Group, High Data Rate (HDR) Duplex, and Low Data Rate (LDR) Duplex.

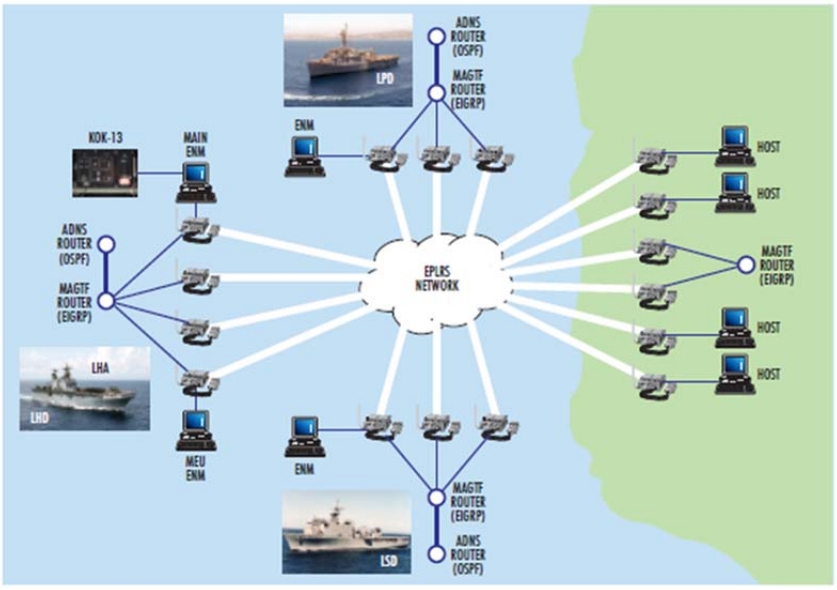

Figure 8. Example of Joint Service Deployment of EPLRS (from Tharp & Wallace)

3. JNN/WIN-T

The Joint Network Node (JNN) is the common name given to the collection of tactical voice, video, and data communications systems that are currently being used by the United States Army. It was designed specifically to meet the Army's need to have a high degree of flexibility and mobility in tactics and communications in combat environments in which information exchanges are very time sensitive and quickly analyzed (Ackerman, 2007). These demands were fulfilled with the JNN's suite of equipment, which consists of a mixture of specialized and COTS components housed in transportable shelters and multiple transit cases (Global Security, Joint Network Node (JNN), 2011).

The JNN suite has the capability to establish a robust network, with interfaces for both terrestrial and satellite transmission sources, and is designed to give commanders and network managers the ability to exercise adjustable control of all communication links and trunks in a deployed environment as mission and the situation dictate. The overall JNN collection is comprised of five major nodes, along with supporting nodes, transit cases, and different satellite terminals associated with establishing local and wide

area connectivity. Compatibility with legacy systems is important for transition as well as communication with forces using antiquated systems. These nodes are located in the United States Army within Divisions, Brigade or Brigade Combat Teams (BCT), and Battalions (Global Security, Joint Network Node (JNN), 2011).

There are three major increments of the Joint Network Node Network (JNN-N) collection that are either in production and use or slated for future development and test iterations. Within each increment, changes and enhancements have been made over time to integrate new equipment, as well as to test equipment destined for implementation in later increments (General Dynamics, 2011).

In recent years, the JNN initiative was integrated into the U.S. Army's Warrior Information Network-Tactical (WIN-T) program. WIN-T was once a concurrent tactical communications program separate from JNN, but the two eventually merged for fiscal and management reasons. Both programs were designed to integrate emerging Internet protocols in order to make "progress toward a fully networked force" (Ackerman, 2007, p. 1).

The WIN-T program is extending the functions of the JNN program with modified assemblages and integration of other emerging technologies into the architecture, such as unmanned aircraft systems (UAS) and components to provide in-depth, out-of-the-box security for client devices. There is focus on the growing concerns of information assurance and extending the network with mobile, self-reliant, and adaptable network components mounted in tactical vehicles. The use of evolving COTS components is expected to continue rather than devising modules purely for military application (General Dynamics C4 Division, 2011). Figure 9 shows the major assemblages aligned with current Army force structure and the various types of data connections between them.

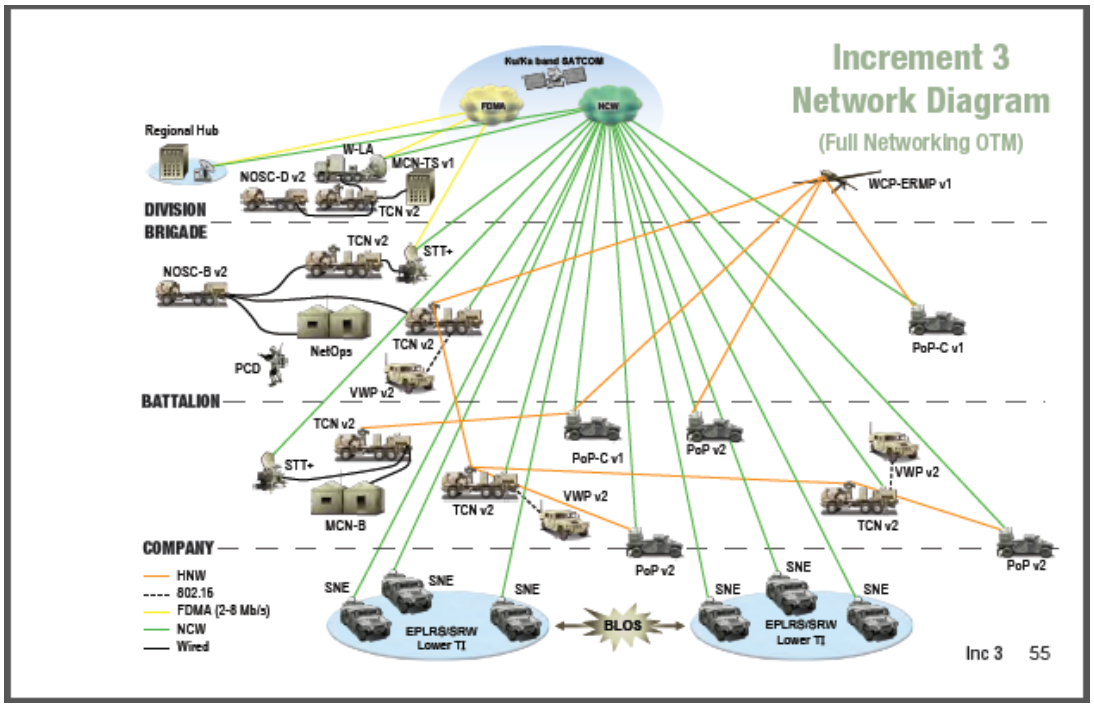

Figure 9. Comprehensive View of WIN-T, Increment 3 (from General Dynamics C4 Division, 2011)

4. Installation as a Docking Station

Installation as a Docking Station (IADS) is a newer focal point of Army tactical networking. The premise of IADS is to assimilate tactical communication nodes with daily garrison operations in order to offer more training opportunities for operators within staffs at the Brigade level and higher. Merging the two environments is meant to bring synergy for staffs and commanders in preparation for upcoming deployments and missions. The mission control systems (intelligence, command and control, etc.) that are used by Army personnel in tactical environments are integrated into headquarters buildings and in offices used in garrison environments. This reduces the need and cost of deploying them, along with the supporting attributes like fuel, while allowing daily use of the systems in preparation for use in real-world scenarios. Through additional network components, service agreements, and coordination with garrison network maintainers (local Network Enterprise Centers (NEC)) and military network administrators, the fusion of their respective heterogeneous systems is feasible (Ackerman, 2007).

The introduction of IASD has come after much analysis of skill retention, training costs, and operator proficiency. It "emphasizes the importance of the program for readiness and preparedness, especially in the case of an immediate-response deployment. Units not finished with their exercises will be equipped with the necessary skills to operate the systems in-theater because they have worked with them all along back home" (Boland, 2012, p. 6).

5. Wearable Tactical Networking Gear

The basic concept of wearable tactical networking and communications gear is not new. Over the years, several countries have devised systems comprised of wearable components with the goal of providing optimal situation awareness and portable communications between all unit levels; the goal is to share the same common operational picture from the higher echelons of leadership to dismounted troops (Turner, Carstens, & Torre, 2005). Both militaries and private companies developed these systems with wired components that transmitted voice and data over combat net radio frequencies. These systems had varying types of security and peripheral components. Some systems are no longer in existence due to issues that include cost, usability, and loss of applicability, while some are still in development. One of the best-known systems of this type is the Integrated Digital Soldier System (IDSS), which was developed by Cobham Defence Communications (Cobham Defence, 2014). The U. S. Army has a similar system that is being developed as part of the Future Force Warrior project (Defense Update, 2007).

As stated earlier, optimal command and control as well as better common operational pictures are desired by soldiers and commanders when on the battlefield and within tactical environments. Technologies such as Blue Force Tracker and Unmanned Aerial Vehicles (UAVs) result in a plethora of ways to disseminate and receive information to and from a unit's headquarters. A problem is that access to these systems is generally limited to the headquarters or soldiers mounted in vehicles. The primary focus of some of the wearable tactical gear programs, as depicted in Figure 10, was to get the same common operational picture displayable to soldiers via a controller or computer

integrated into his or her gear along with the ability to share his or her situational awareness with nearby unit members and with headquarters elements by means of various wearable devices and sensors. Mobile devices (cellular phones and tablets) are a preferred means of meeting these goals due to their increasing processing power and portable sizes (Defense Update, 2007). It is reasonable to expect that 802.21-enabled devices may one day be a part of some of these initiatives due to their ability to connect to multiple types of network access media.

Figure 10. Representation of Experimental Future Force Warrior Uniforms (from Bonsor, 2005)

D. MOBILE ELECTRONICS IN MILITARY OPERATIONS

1. Current Use

Cellular phones and smartphones have been in the military inventory for years. It is commonplace to see various leaders with Blackberry devices, utilizing them as necessary for command and control as well as for functions such as checking enterprise email. They can be found in use in both garrison and tactical environments. iPhones and iPads were not allowed for use in government and military networks due to security concerns. A new security technical implementation guide (STIG) was released during the summer of 2013 allowing for government-issued Apple products to access Department of Defense networks (Army Times, 2013). Personal mobile devices, regardless of vendor, are not allowed on government or military networks; however, the newer Blackberry 10

OS, Apple iO6, and Android 2.2 devices have been approved for future use. The STIGs, named for each of these mobile operating systems, were released in 2013. Progress has been made to factor in security in the operation of these devices on government networks. "The Defense Information Systems Agency is working to set up a Mobility Device Management system to securely manage all mobile devices with access to DOD networks" (Army Times, 2013, p. 4). Specifically for tactical environments, it is routine for units to acquire Thuraya satellite products and Global System for Mobile (GSM) phones utilizing multiple commercial vendors to extend unclassified command and control in a theater of operations.

Budget restrictions and fiscal management changes brought about a reduction of the Army's mobile device footprint limiting allocations to key leadership positions or deemed as necessarily critical priority for mission command and control. Meanwhile, specialized testing units including Network Integration Evaluation (NIE) units, such as 2nd Brigade, 1st Armored Division, as well as independent vendors seeking to enter government and military markets, have conducted pilot testing for ruggedized and multi-service devices. At this time, there is not a widely-distributed and used cellular architecture in the military designed for tactical use.

2. Future Use

There are numerous initiatives currently that are designed to assist data transmission during military operation. Some of the concepts of these initiatives either resemble or are relevant to 802.21 technologies. Pilot programs, such as MACE and the Future Forces Warrior, have been tested extensively in recent years. There are several other devices undergoing testing in controlled tactical environments and field exercises, as well as during operational deployments. Specialized applications are usually developed to function as a tool to support military operations. The importance of using intelligence, surveillance, and reconnaissance (ISR) in previous wars has driven collection and information sharing to be explored in more portable aspects.

Two applications that were tested in the recent past are the Joint Battle Command-Platform (JBC-P Handheld) and the Tactical Ground Reporting (TIGR)

Mobile. JBC-P is a condensed, mobile version of the vehicular Force Battle Command XXI Brigade and Below (FBCB2) which is used to show maps, key geographical terrain, enemy locations, and locations of friendly forces. TIGR Mobile utilizes multiple ISR databases to disseminate information. “JBC-P displays a map of the battlefield, using GPS to indicate the locations of friendly forces, enemies, and landscape hazards in real time. TIGR allows soldiers to send photos back and forth, and swap historical information relevant to the operation” (Coxworth, 2011, p. 3). Services such as GPS and client authentication, re typical features that are expected for military application along with multiple display modes and encryption options.

Increment 3 of the WIN-T initiative includes a Personal Communications Device (PCD) (shown in the figure below) that is in development. It would be operational worldwide utilizing commercial frequencies (General Dynamics C4 Division, 2011). Also, the National Security Agency has done extensive work in formulating a secure “approach for using commercial devices and networks to securely connect mobile users to the Government enterprise” (Information Assurance Directorate, 2012, p. 1).

Figure 11. Image of a WIN-T Personal Communications Device (from General Dynamics C4 Division, 2011)

E. CHAPTER SUMMARY

The information in this section provides background regarding past, current, and future communication technologies, both large network technologies and mobile technologies that are or may be employed by military personnel. Each technology discussed has relevance to the emergence of the 802.21 standard and tactical deployments. Expansion of capabilities, along with the desire for broader data access and fast reliable services, continue to call for consideration of the adoption of mobile COTS technologies. Security concerns and inconsistent service handovers affect the possible use of 802.21-enabled devices on a wider scale. Tackling these issues may provide a means to address some of the roadblocks to greater assimilation of these technologies. Fluctuating federal budgets and difficulties with devices authenticating to mobile base stations affect the wide use of these devices in tactical situation. The next chapter addresses one of the issues that affect widespread use of 802.21: mitigating data loss during system hand-off.

III. PROPOSED CONCURRENT BUFFERS AND TACTICAL NODE PLACEMENT

We propose two objectives with respect to 802.21 implementation: a measure to assist in seamless handovers and a solution for tactical employment. Both ideas were developed after researching the MACE initiative and discussion of future implementations. This chapter discusses the basis and research behind both ideas.

A. ISSUES WITH HANDOVERS IN 802.21

As discussed earlier, a number of issues exist with handovers in the context of 802.21. A summary of the issues is as follows:

1. Handovers may not be successful, leading to interrupted network access
2. Lack of an ability to guarantee seamless handover functions without losing data
3. Optimum service decisions may not be accurate
4. Securing data-at-rest
5. Scalability and interoperability
6. Hidden and exposed node problems may arise
7. All data access providers do not follow the same configurations for their services

B. PROPOSED CONCURRENT BUFFER IN 802.21 DEVICES

To address the issues of data service handover (MIH) during heterogeneous system transfer, we recommend the incorporation of an additional buffer in the MIH protocol stack allowing for two identical instances of data to be simultaneously available as the handover services negotiate the preferred service based on availability, signal strength, and other parameters. Implementing such a solution requires sensitivity to potential issues that might be raised due to an implementation of shared or multiple buffers, such as data consistency, protection of data at rest and resource usage.

1. Use of Data Buffers in Mih Stack

Currently, within the IEEE 802.21 standard, there is a data buffer associated in the preparation of service handovers to minimize the possibility of lost data packets (Taniuchi et al., 2009). This is definitely helpful for homogeneous networks but does not

fully address interactions between heterogeneous networks. The single data buffer is for a single interface (in a mobile device) to allow the retransmission of previous data packets in the event of a connection handover in a homogeneous network. The MACE initiative has done extensive development regarding how the buffer operates and how data stays secure while in the buffer. The current software of a device in the MACE architecture has a Duplicate Packet Detection cache (DPD) that allows the multicast forwarder to be mindful of which data packets have already been forwarded and may cause integrity or consistency problems when previously forwarded packets are seen at other interfaces (Applied Communication Sciences, 2012).

Most 802.21 user devices have at least two interfaces (e.g., WiFi and WiMax) so that handovers can be affected as the environment changes. We propose incorporating one data buffer per interface to prevent data packet losses during heterogeneous service handovers. The active service would have to duplicate the data in its buffer and send it to the buffer of the inactive interface in preparation for possible handover, in effect creating a “hot stand-by” mode.

Whether the duplicated data would be sent to the secondary buffer continuously or periodically would necessitate consideration and technical exploration beyond the scope of this thesis. Herein we propose the secondary buffer begins to receive duplicated data depending on the link state of each of the interfaces. For example, if a WiMax interface is secondary on a device, due to design or preference, and that interface is reporting an available or optimum service nearby, the current service may begin to duplicate its data before the final decision for a handover is reached. The same would apply if the primary interface were experiencing degraded service or if the device is moving away from the service provider assets.

The need for additional buffering is derived from the complexity of service handovers in heterogeneous networks. “Handoff involving heterogeneous access can take place in many different ways, depending upon the activity of the second interface. In one scenario, the second interface comes up when the link to the first interface is down. This scenario usually gives rise to undesirable packet loss and handoff delay. In a second scenario, the second interface is being prepared while the mobile still communicates

using the old interface, and at some point the mobile decides to use the second interface as the active interface. This results in less packet loss as it uses make-before-break techniques. In [a] third scenario all the required state and security associations (e.g., PPP state, LCP, CHAP) are established ahead of time thus reducing the time taken for the secondary interface to be attached to the network" (Dutta et al., p. 7).

The initial literature and related research review conducted shows that, in theory, adding an additional buffer to 802.21-enabled devices is feasible and may assist in handovers. After several discussions with representatives from Applied Communication Sciences, it was further validated that using an additional data buffer with duplicate data was indeed a viable solution. Originally, implementation of modifications to the protocol stack in order to set up for later testing. However, discussions with Applied Communications engineers led to the conclusion that such a modification, although feasible, would perhaps take a relatively long time to design and implement.

It is not desirable to modify the majority of other functions currently incorporated in a MACE network to achieve concurrent buffering. We suggested incorporating two DPDs, one for each interface, to be monitored by the MFE slightly differently than the single one. The buffering process would not affect the aspects of a handover operation that govern when a service handover occurs, with the same applying to MDG-to-end user device interaction or the function of the Media Independent Event Service. However, it is possible that battery life, processing power, and other components may be affected in a manner similar to the way that battery charge is drained as a device searches for a nearby antenna. This would require further exploration prior to adoption of the added buffers as a final design change. This particular exploration is beyond the scope of this thesis, which intends to offer a design idea for such duplicate buffering, leaving verification of its practical viability due to side-effects to further study.

Appropriately sizing the buffers must take into consideration several factors including storage capacity, compliance with standards, costs, and processor speed as these vary per mobile device model and manufacturer. The additional memory needed to implement our proposed buffer scheme could be implemented in the Multicast Forwarding Engine described in Chapter II.

2. Security Concerns

One of our concerns was to ensure that the data stored in the suggested buffers was secure. We did not want to introduce vulnerabilities by having a copy of data that was not necessarily secure as handover decisions were being executed. Our discussions with ACS included attacks aimed at extracting data while it resided in the concurrent buffer, as well as the best way to encrypt the duplicate data as required prior to possible handover, lead to the solution idea that we proposed.

The suggested solution addressing a possible security issue includes incorporating slight modifications to how MACE uses multiple IP addresses and headers in its current configuration to manage multiple interfaces, devices, and even MOBIKE utilization. The suggested solution involves the HTG and end-user devices.

Figure 12 shows the logical hierarchy of IP headers and their mapping to interfaces in the MACE setup. The IP addresses are explained thoroughly in MACE's Phase 1 System/Software Design Description. "At the lowest layer is the Temporary IP address (TIP) which is the IP address of the physical interface of the device. The overlay has a Virtual IP Address (VIP) for which no explicit interface is created. However, all packets that are part of the overlay have the VIP that resides on top of the TIP. The Permanent IP Address (PIP) is implemented as a GRE end-point which rides on top of the VIP. Both the PIP and the VIP are immutable addresses that do not change" (Applied Communication Sciences, 2012, p. 6).

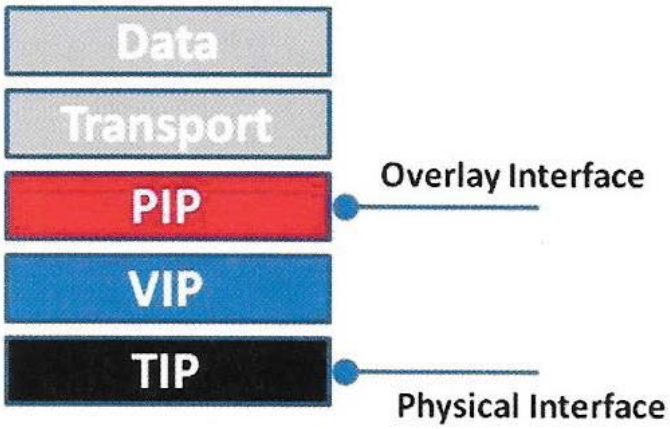

Figure 12. Logical Hierarchy of IP Addresses in MACE Software (from Applied Communication Sciences, 2012)

Our proposed strategy for addressing security for a duplicate data buffer involves the fact that the VIP does not apply to a particular interface of a device. We suggest that each physical interface be configured to have a distinct virtual IP address included in its logical hierarchy compared to having only one that is not necessarily used by any interface. Likewise, the HTG would need multiple VIPs registered (one per physical interface) for each device's temporary IP address as it associates and disassociates with them. The communication between the MDG and an end-user device includes updates to an accompanying IP address (or VIP in this scenario).

MOBIKE and GRE functions would not change since the PIP of the device would not change, but it is assumed that the active VIP in the end-user device may need to change just prior to the service handover. According to MACE's documentation the HTG and end-user device "agree with a pair [of] VIP addresses for the GRE tunnel. Each HTG sets up a tunnel interface during its initiation and uses the tunnel interface as its own VIP" (Applied Communication Sciences, 2012, p. 11). HTG is sometimes preloaded with known PIPs and VIPs of devices within a particular network that may connect, or this information is shared during the beginning phases of assessment and authentication. Manipulation of the PIPs and VIPs would allow the multiple interfaces to communicate securely without regard to service while maintaining the previously established security parameters. Figure 13 shows the current logical hierarchy without detailed information of

IP headers, checksums, etc. Depending on the how the PIPs and VIPs are modified and processed, security can possibly be increased compared to the default preloaded set.

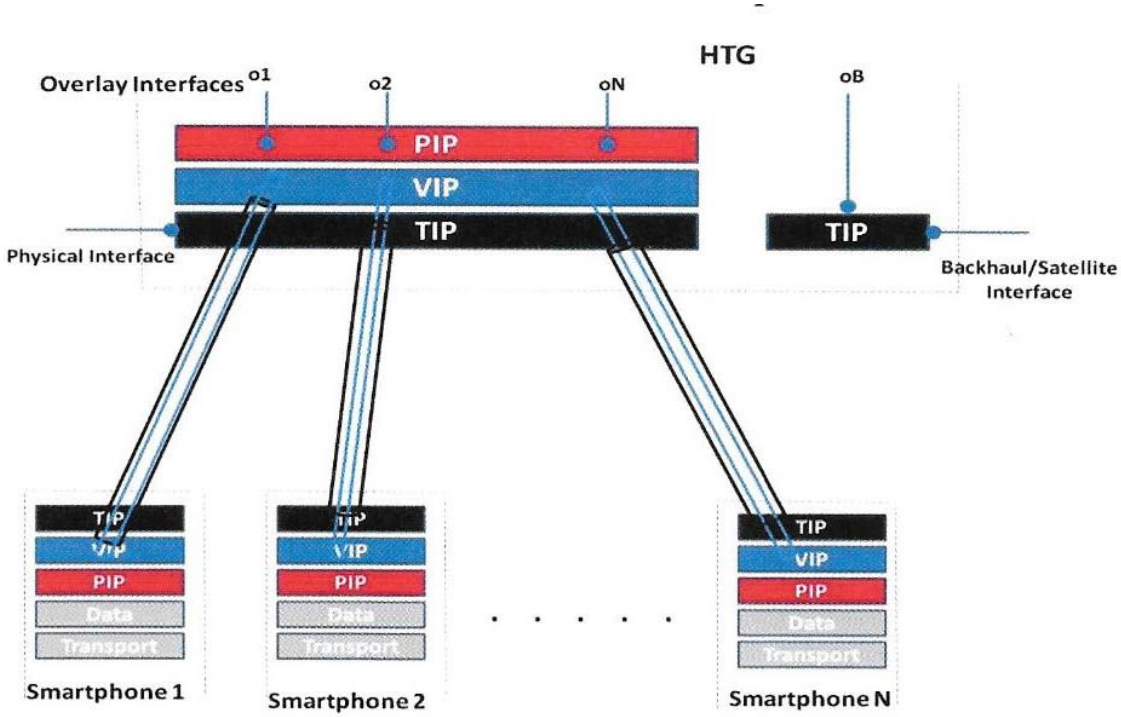

Figure 13. Logical Hierarchy of IP Addresses for Multiple MACE Devices (from Applied Communication Sciences, 2012)

B. MIH NODE PLACEMENT IN TACTICAL ENVIRONMENTS

1. Issues with Tactical Use of 802.21

In contrast to the commercial sector of network service provision, the network nodes and components of tactical networking service providers and units are possibly as mobile as the devices that will pull services from them. The communication assemblages and transportable antennas used by military units are designed to be deployed and moved easily and expediently to necessary locations in tactical environments. This means potential network discontinuities may occur when segments of the network are shutdown to support relocation. This poses additional problems for the use of tactical mobile devices, as they draw services from tactical networks instead of or in lieu of more stable or permanent commercial networks, for example those from Sprint and AT&T.

Previous research in utilizing 802.21 technology in tactical environments supports the aforementioned. “In a tactical environment, the infrastructure points (e.g., HTG) are mobile. Information needed to support handover decisions could be dynamic and mission specific. Moreover the formation of ad-hoc mesh networks are dynamic and subject to user mobility patterns and communication” (Applied Communication Sciences, 2012, p. 11). Consideration of mobility of users is critical in planning for deployment of 802.21 networks in tactical environments. End-user devices hardened for tactical use, as well as commercially available devices that may pull services from military networks, are either in use or being tested for future use.

If tactical end user devices (cell phones and tablets) are to be used reliably on the battlefield, military communication personnel and commanders will have to consider the capabilities and limitations inherent to these technologies as well as to consider terrain, allocated frequency ranges (when in foreign lands), and data security. The impact of such issues on military tactical networks is explored by considering the performance of the Enhanced Position Location Reporting System (EPLRS).

2. Use of EPLRS Networking Scheme With 802.21

The MACE program’s mission is to provide a mobility management solution that “addresses the challenges of retaining best possible communication links while the system is on the move, and at the same time performing seamless session handover without sacrificing the requirement of multiple layers of security” (Applied Communication Sciences, 2012, p. 2). As described earlier, the solution incorporates multiple nodes, servers, software adaptations, etc. The second objective of this thesis is proposing a mobile node solution similar to the now antiquated EPLRS.

The position reporting functionality of EPLRS was developed such that it could be used as a backup to Global Positioning System (GPS) when there is a situation where GPS is either not available or not operating suitably. EPLRS may not give precise positioning, but it is within an acceptable margin of error. We suggest a system similar to EPLRS, while incorporating some of its fundamental properties, to be utilized in 802.21 networks. Nodes with capabilities similar to EPLRS will be in communication with each

other informing one another of the status of known nodes, that is, which ones are nearby, active, or degraded. Layer 3 devices, such as routers and some other network devices, perform similar functions.

Incorporating positioning and location functionality into the mobile stations or base stations utilizing 802.21 networking may provide valuable capabilities for emerging tactical networks to include virtual-circuit based needlines. The self-healing nature of EPLRS would be ideal for modeling tactical environments that may employ 802.21 technologies, since the nodes may relocate or operate on the move.

Whether for tactical vehicles or command centers, utilization of similar technology in these nodes would permit nearby base stations or mobile nodes to be constantly updated. The base station and mobile nodes would, in turn, exchange network information. This could save battery life and processor activity in end-user devices by taking some of the handover decision making activity out of the device while relying on its active interface to continue receiving status information.

Also, the OTAR function of EPLRS, or something similar, might be applied to 802.21 networks to distribute encryption keys or seeds for encryption algorithms for devices and nodes. This may allow devices that had not been pre-authorized to join an existing network. Some Heterogeneous Tactical Gateways (HTGs) in the MACE implementation of 802.21 come preloaded with the IP addresses, etc., of devices known to be in their respective networks. In a tactical environment, devices from neighboring units may come in and out of various established networks. The OTAR functionality would be a way to authenticate devices encountered through such opportune encounters to share information securely.

C. CHAPTER SUMMARY

This chapter covered two proposals to address performance and deployment issues of 802.21 networks. The first suggested a measure to assist in seamless handovers by adding one or more buffers that would prepare data for transition from one service provider to another. The second discussed a recommendation for tactical employment by

suggesting that major tactical radio nodes be used to assist in regulating 802.21 handovers, with self-healing and notification properties similar to EPLRS networks.

The next chapter describes an experiment meant to simulate mobile 802.21 nodes and devices that are constantly moving in a particular geographic space. Using the SPEED software system, simulated nodes, both mobile and stationary, are configured utilizing the frequencies and properties of other networking technologies such as WiFi. The intent is to test and observe simulated node interactions in order to: 1) experiment with proper node placement in tactical environments, and 2) to demonstrate how a self-healing network topology may be useful in 802.21 implementations.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. BUFFER IMPLEMENTATION AND MOBILITY EXPERIMENT RESULTS

As discussed in Chapters II and III, service handovers in 802.21 networks are unreliable. To address this issue, we propose to incorporate additional buffers in the existing MIH protocol stack that will securely buffer duplicated data as preparations for handover occur. The risk of data loss in heterogeneous handovers poses significant concerns for tactical users. The additional buffers are offered as a way of mitigating such loss and associated performance degradation.

Section 3.B contained an analysis of the feasibility of facilitating such a buffer. Further analysis was done to consider whether a buffer as described would be robust enough to prevent vulnerabilities or issues as the service changed over to a more preferred network. A preferred network can be defined as one which is more stable and efficient or as dictated by policies (access, restrictions, etc.) that may be instituted in the end user devices.

Without access to 802.21-enabled devices and networks, we decided that simulating the tactical environments, frequency ranges of common communication services (Wi-Fi, WiMax, etc.), and mobile antennas would be useful for demonstrating the need for managing handovers in tactical employments. Using two network simulation programs, a notional tactical networking environment was created to explore the impact of node mobility on wireless users, particularly with respect to proposed node placement using technology similar to EPLRS. It is expected that 802.21 networks incorporating some of the positive attributes of the EPLRS networks would be helpful in mitigating the impact of expected movement of nodes and units on an actual battlefield.

To provide context, the parallel buffer concept is further explained prior to presenting the simulation methodology and results.

A. THE BUFFER CONCEPT

The inability to guarantee consistent handovers presents possible terrain-induced denial of service scenarios. Earlier, a “hot standby buffer” was mentioned, which consists

of an active network interface duplicating the data in its buffer and sending it to the buffer of the inactive interface in preparation for possible handover. The overarching concept of this thesis is to explore the feasibility of an additional or "hot standby" buffer. Our basic approach is to maintain one additional buffer per accessible network service on the device. As handover functions occur in the election of a preferred or optimum service, the buffers store data packets from the master data buffer in order to prevent data loss.

Figure 14 shows how additional buffers could be implemented in the existing TCP/IP protocol stack on an 802.21-enabled device. Transmission Control Protocol (TCP) buffers are shown in the image only as the connectionless nature of the User Datagram Protocol (UDP) does not account for reliable data transfer. If UDP data is to be sent, the active application within the device would handle the transmission of data implementing its own buffering, if applicable. Such is typical for any application-layer entity electing to use UDP while still maintaining a requirement for reliable data service. (One such application is the Trivial File Transfer Protocol, TFTP.)

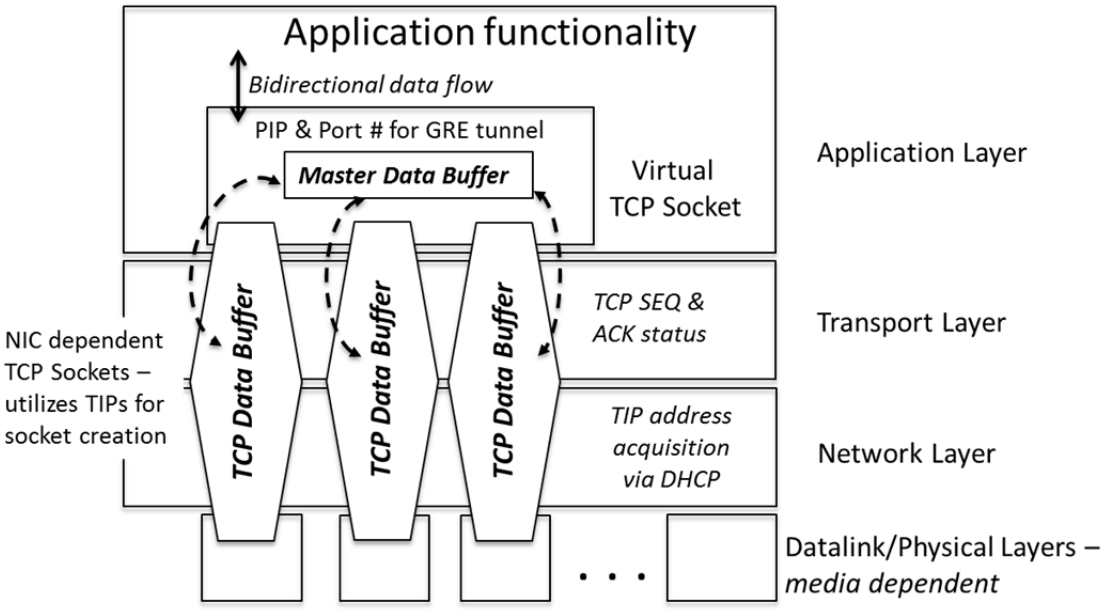

Figure 14. Proposed Buffer Concept

The concept incorporates the Temporary Internet Protocol (TIP) and Permanent Internet Protocol (PIP) addresses as seen in the MACE implementation. The premise of the concept is to incorporate and synchronize cooperative TCP buffers, each supporting an underlying physical interface, in order to mitigate possible data loss during handovers.

Each end-user device has multiple network interface cards (NICs), or their equivalent, on the system integrated circuit board or chip set, one for each service employed for the device (WiFi, WiMax, etc.). Each of these interfaces has a TIP associated with it. These are used for socket creation and possible security functions, such as further encryption of buffered data, if needed, and are employed by the underlying network access service. The device has only one PIP, which is associated with the device, and it is also used by the application interface that is receiving and transmitting data. The PIP is used for establishing the GRE tunnel within the application layer as part of a virtual socket, as well as for any application-to-application authentication scheme designed into the service.

The proposed master buffer is continually buffering and managing data as that data is received or transmitted. The parallel TCP data buffers, each associated with a particular interface, interact with the master data buffer either when its governing service is active or an interface is being prepared for an upcoming service handover selection. Figure 15 shows how each interface interacts with the master buffer during handover operations. The virtual socket manages the master data buffer in the same way a TCP socket manages its reliable data transfer process through exchanges of sequence numbers indicating the status of outgoing streaming data (byte-flows) and acknowledgment numbers indicating the status of incoming data (byte) flows. Since the actual sequence and acknowledgement numbers are generated and transmitted by the actual TCP sockets, these values must be coordinated between the virtual socket and each of the actual TCP sockets. This would require the virtual socket to maintain a look-up table to allow for consistent reference to the master data stream and the underlying TCP sockets.

The premise is that device’s connected interfaces are actively receiving data packets to be processed by the device and transmitting data packets through the network service to which it is connected on behalf of the application to which it is bound. The

interfaces are not actively exchanging packets unless a pending service handover election is occurring even though it may be receiving a duplicate of the data being buffered. When nearby networks with services different from that of the active service are identified during other MIH functions, the buffers associated with them become active and begin receiving duplicate copies of data packets from the master data buffer in preparation for an inactive and the data buffer associated with it no longer exchanges data with the master buffer. The newly elected interface and service conducts transactions with the remote host on behalf of the virtual socket and its associated PIP pending handover. After a handover is completed, the former active interface becomes inactive and the data buffer associated with it no longer exchanges data with the master buffer. The newly elected interface and service conducts transactions with the remote host on behalf of the virtual socket and its associated PIP.

Figure 15 shows the four phases of a service handover in an 802.21 device with a focus on the use of the incorporated buffers. Figure 15a shows only one active interface and the device is receiving (or transmitting) data. It is labeled “Pre-Handover Operation,” as the other functions involved in an 802.21-device are not occurring. Figure 15b shows a second buffer associate with a particular service being prepared after a network utilizing that service has been detected. Figure 15c shows the status of each of the service buffers after a successful service handover. The previously active buffer still receives data packets as the connectivity for the new service is verified and conversion to the newly activated interface is completed. Figure 15d is similar to Figure 15a except that the device is transmitting and receiving over a different interface and service.

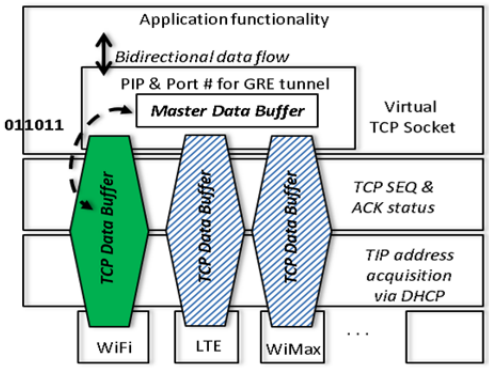

Figure 15a: Pre-Handover Operation

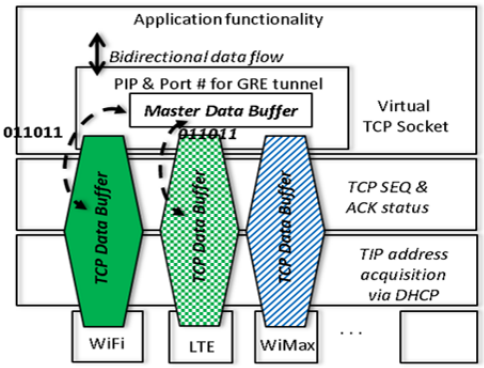

Figure 15b: Handover Preparation

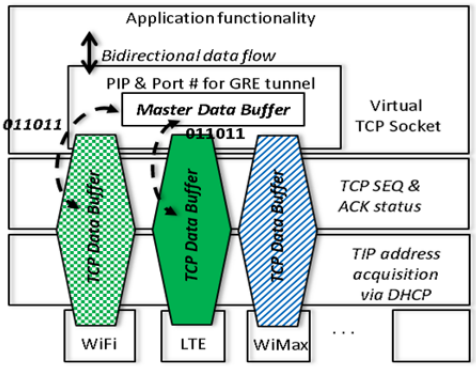

Figure 15c: Handover & Verification

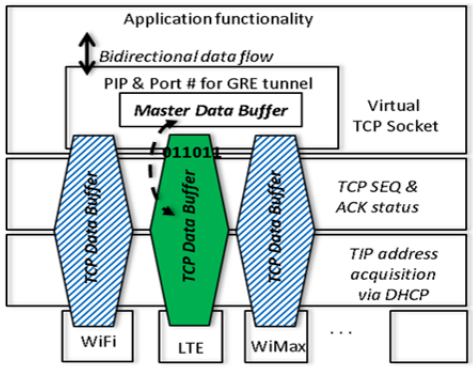

Figure 15d: Post-Handover

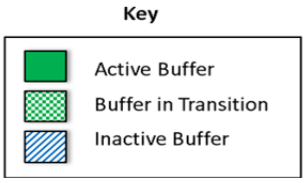

Figure 15. Handover Process With Additional Data Buffers

Though only three buffers for three heterogeneous services are shown in Figure 15, many more could be incorporated. This even includes multiple buffers for homogeneous network handovers such as multiple WiFi (802.11) networks with different network identifiers (SSIDs). Also, multiple "hot standby" buffers, other than the one associated with the active interface, can receive duplicated data packets in preparation for a handover compared to only one as shown in Figure 15. There may be instances in

which preferred interfaces and services may be pre-configured necessitating preparation of more buffers.

Figure 15 showed an overview of the functionality of the proposed buffers, but there are some details requiring further explanation. Underlying TCP sessions involving the additional buffers and the temporary IP addresses would occur simultaneously while a virtual TCP session between the end-user device and connecting server is operating. The virtual TCP session must be designed to keep the data stored in the actual underlying TCP buffers synchronized and prepared in case of a service handover. The virtual socket serves as the application programming interface (API) for the application itself.

Instead of the client-server communication involving a single active (TCP) network connection, the master buffer serves as a virtual session between the two end-device applications, the additional buffers provide the actual connection-oriented session between the two devices or hosts, coordinating their data streaming with their associated master buffer. The underlying TCP sockets support the virtual socket handling 802.21 handovers. The TIPs and service ports make up the sockets for the additional buffers. As the port numbers and the PIPs (of the device and master buffer) associated with the two end-points of the virtual socket ensure consistent connection between the two application entities, the underlying TCP sockets are not constrained by the IP address or port numbers used by the virtual socket, thus they can utilize the TIP associated with the real physical network devices and the standard port number of the service. The sockets are opened and closed to maintain contact between the two hosts to keep the data consistent in each of the active TCP buffers as well as with the master buffer within each host.

As each underlying TCP socket will establish its sequence numbers and associated acknowledgment numbers randomly during the session set-up (TCP three-way handshake), the virtual socket must translate the associated references to the actual TCP data streams with the original data stream as managed by the virtual socket. For example, the active service may initiate data transmission with a server process with a sequence number starting with 100 for the data packets moving through the master buffer. However, the other TCP buffers may begin their sequence numbers with 275, 310, etc.; further, since these streams may be initiated at any time, the first bytes buffered by them

may not correspond to the beginning of the application's data. The virtual socket must map the relative position of each TCP buffer's state (sequence and acknowledgment numbers) to the master buffer, which is ultimately the state of the application's data exchange.

The master buffer keeps the other buffers in sync via a sniffer at the data link layer of the TCP/IP networking scheme, where the pertinent fields of the encapsulated IP and TCP headers (TCP sequence and acknowledgment numbers, IP address, checksum, etc.) are extracted from outgoing and incoming session packets. It is also used to manage the virtual sockets of the inactive interfaces. Figure 16 shows the data flow with respect to the networking scheme.

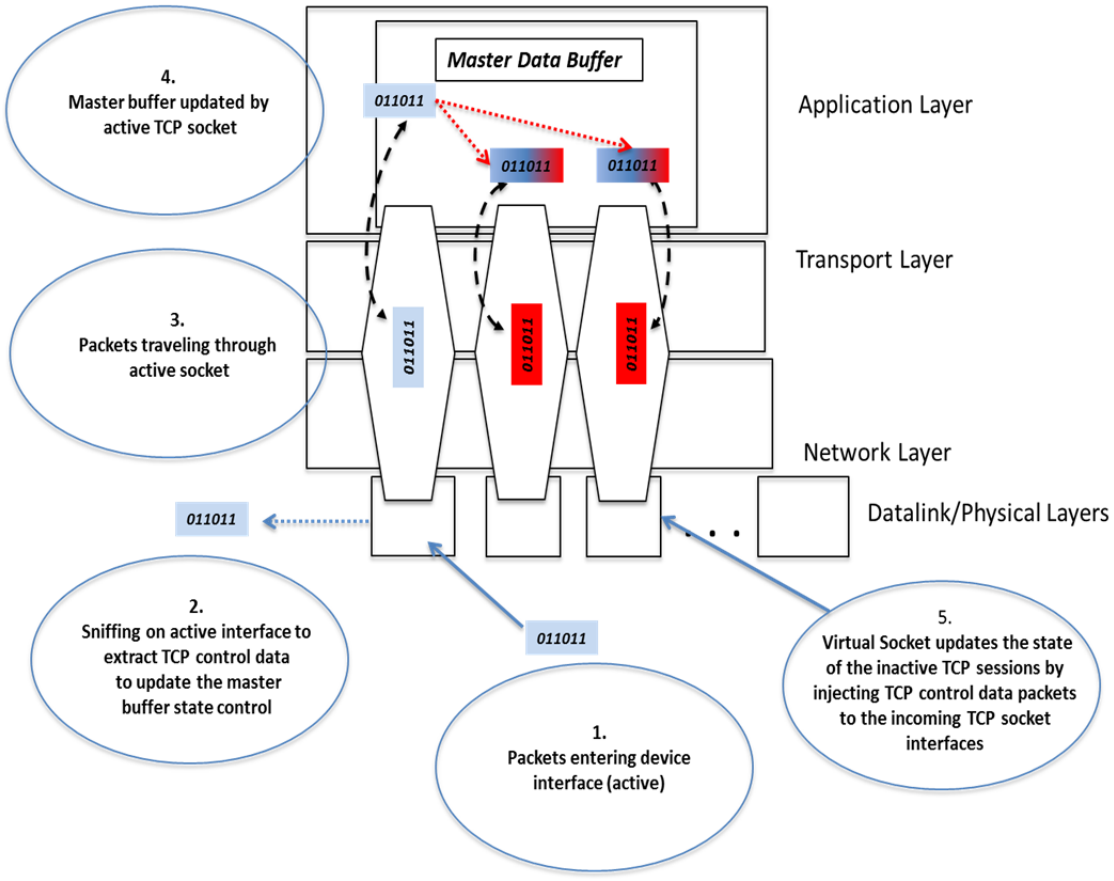

Figure 16. Proposed Buffer Data Flow

It is assumed that data in the individual TCP buffers has already been encrypted prior to submission to the master buffer, using the encryption scheme of the GRE tunnel established as part of the virtual socket between the client and the server. Doing this eliminates the need to encrypt the data packets within the additional buffers and simplifies the concurrency management between buffers.

The proposed additional data buffers may only address some of the handover issues in 802.21 networks. Mobility requires reliable handover functionality in a tactical 802.21 network. In tactical environments, the antennas and base stations may be mobile along with the devices. This is in contrast to most commercial implementations, since in the latter the base stations are typically stationary. The simulation discussed in the next section of this thesis addresses mobility of devices and nodes and the appeal of service handovers as provided for by 802.21 networks.

B. SIMULATION SETUP

Though the additional buffers are proposed to make more reliable networks, the impact of mobile nodes and end-user devices needed additional consideration and focus. The problem underscores why reliable handover functionality is necessary especially in a tactical environment. We could not simulate service handovers with the proposed duplicated buffers due to a lack of 802.21-enabled equipment or adequate simulation software, but we decided to simulate a tactical environment with communication nodes using a simulated 802.21 environment in which multiple data services are used. The issue of mobility was addressed by suggesting a self-healing network and shown by the simulation of mobile nodes mirroring commonly used data access technologies in comparison to EPLRS networks. Showing the difficulty of service handovers with mobile nodes in tactical environments demonstrates why modifications to implementing the IEEE 802.21 standard is needed if deploying the technology is to be successful.

Two different network simulation software packages were used to simulate an EPLRS network and individual technologies that may be integrated into a tactical 802.21 networking scheme. An EPLRS simulation was done with a software program called

System Planning, Engineering, and Evaluation Device (SPEED), and the other technologies were simulated in Radio Mobile.

SPEED is commonly used by United States Army and Marine Corps communications personnel to profile prime links between tactical communication nodes using parameters such as elevation, equipment transmission/reception power, antenna height, etc. It has features such as a separate WiMax analysis, multiple point-to-point (P2P) analysis categories, the ability to overlay multiple map types, etc. SPEED, version 11.1.1, came preloaded with a set of military systems currently in the inventories of the respective services. None of the systems had parameters (frequency range, etc.) close to data network technologies like WiFi, WiMax, etc. Also, the software did not accurately allow the creation of nodes, clients, etc., with the necessary parameters to simulate those technologies. Therefore, a more limited simulation was conducted. SPEED was used to simulate nodes containing EPLRS and systems similar to common data access technologies to show the functionality and benefits of utilizing handover technology in a mobile network. Figure 17 shows the typical console along with simulated nodes on an imported map.

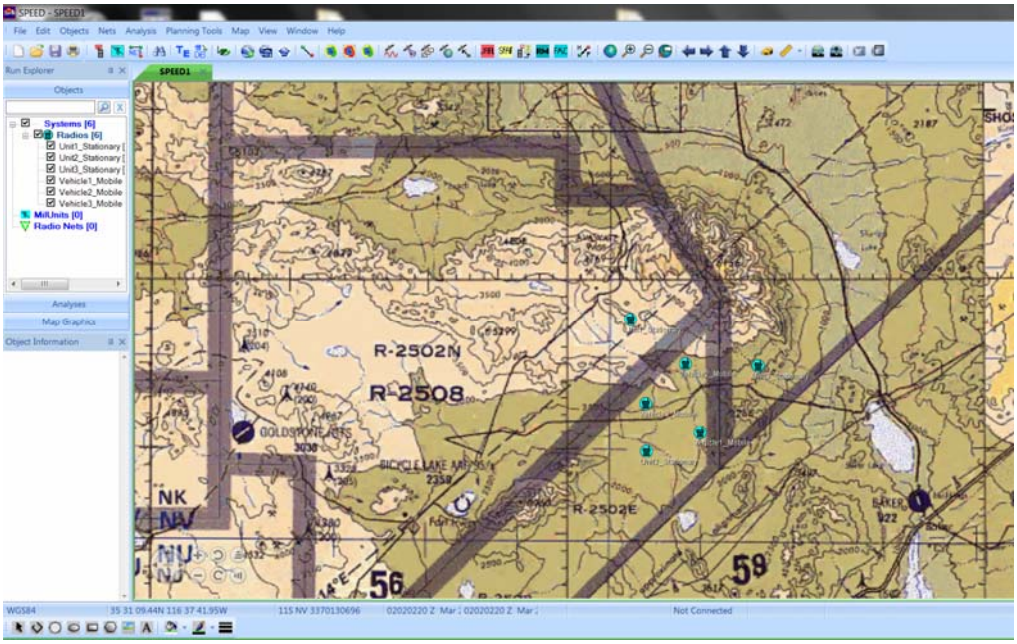

Figure 17. Screenshot of User Console in SPEED

For this simulation, maps of areas within the National Training Center (NTC), Fort Irwin, CA, were used for their similarity to the tactical environments of Iraq and Afghanistan. Maps and imagery were downloaded from the National Geospatial-Intelligence Agency for use in the SPEED program. Both mobile and stationary nodes were created with the intent to simulate how EPLRS radio and networks request and send needlines to keep topology status updated. Figure 18 provides an example of a menu used in SPEED to load specific locations from an imported set of imagery.

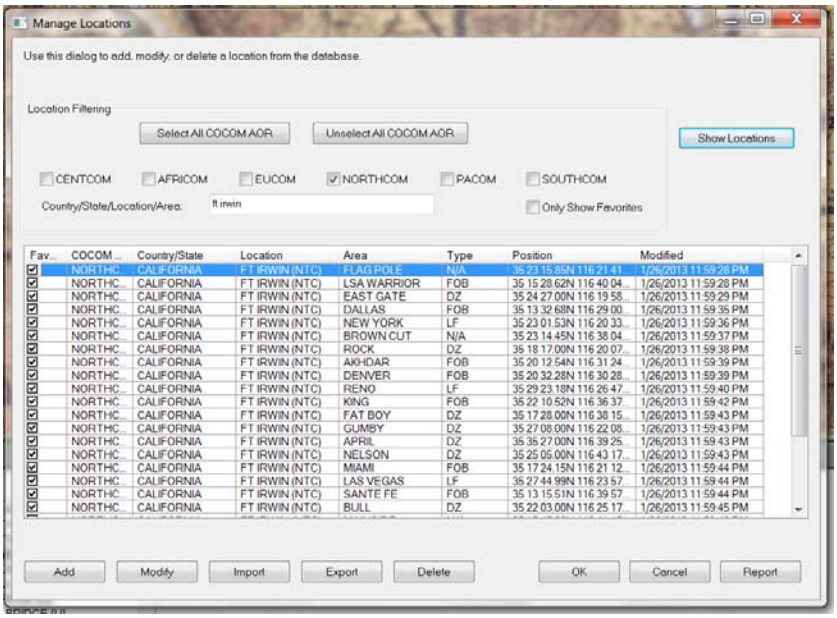

Figure 18. SPEED Map Location Menu

Radio Mobile is a radio propagation and virtual mapping software capable of analyzing multiple types of networks utilizing maps from sources such as GoogleMaps, Mapquest, etc. We used Radio Mobile version 11.4.4 for this simulation using the typical frequency ranges of WiFi and WiMax. As with SPEED, stationary and mobile nodes were created in Radio Mobile, but they were made with parameters and network components typical of WiFi and WiMax. Maps were imported from GoogleMaps to show elevation as well as land features. To keep the locations of nodes consistent between the two different pieces of software, the same longitude and latitude grid coordinates were used in both.

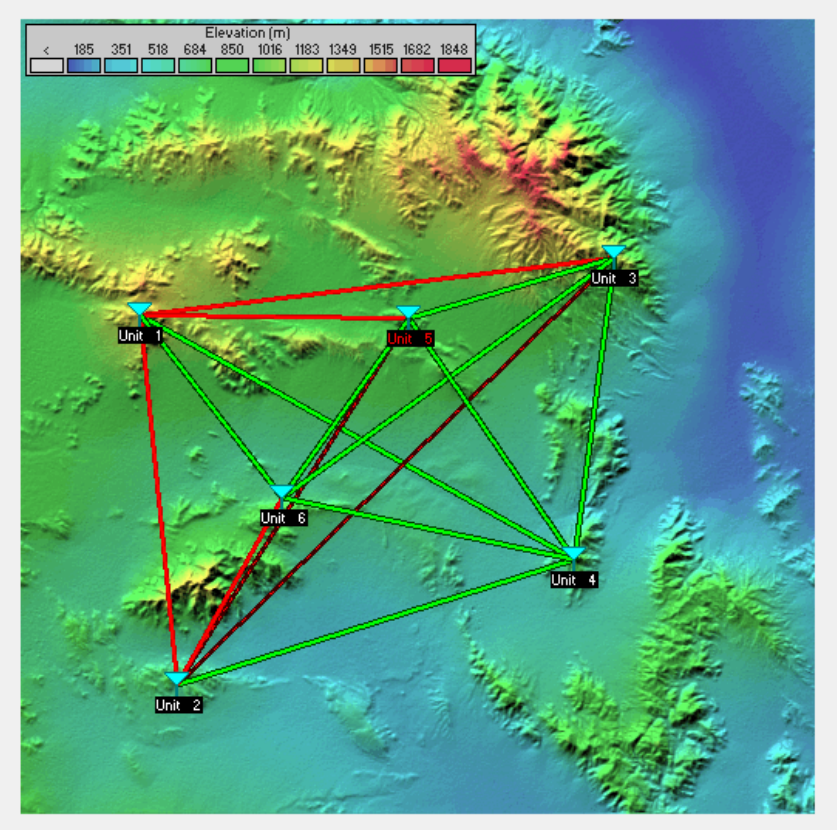

Figure 19. Initial Node Setup in Radio Mobile (20 W Power Setting)

As in SPEED, we created six nodes in Radio Mobile software to simulate three stationary nodes and three mobile nodes. The first simulation for each program analyzed all nodes in stationary positions. Subsequent simulations modeled three of the nodes moving in the simulated environment. Network analysis (signal strength, line of sight, etc.) was conducted for each of the simulated movements. Continuous movement of the mobile nodes was not mapped and analyzed for ease of data interpretation. Instead, the mobility of nodes was modeled piecewise with nodes relocated to other places on the maps before each measurement. Original tests (both stationary and mobile node movements) were conducted with a transmission power of 20 Watts. Figure 19 shows some of the nodes with that transmission power and the connectivity between them as evaluated by the software. Afterwards, additional mobile node movements were evaluated at 100 Watts, for which the higher power setting for EPLRS radio sets is allowed in the SPEED program. The same power settings were applied to the

corresponding nodes in the Radio Mobile software. Figure 20 shows one of the configuration menus used to set the parameters of each node. Table 3 shows the names and characteristics of the six described nodes simulated in both SPEED and Radio Mobile software. WF denotes nodes with WiFi as the primary service, and WM denotes nodes with WiMax as the primary service utilized.

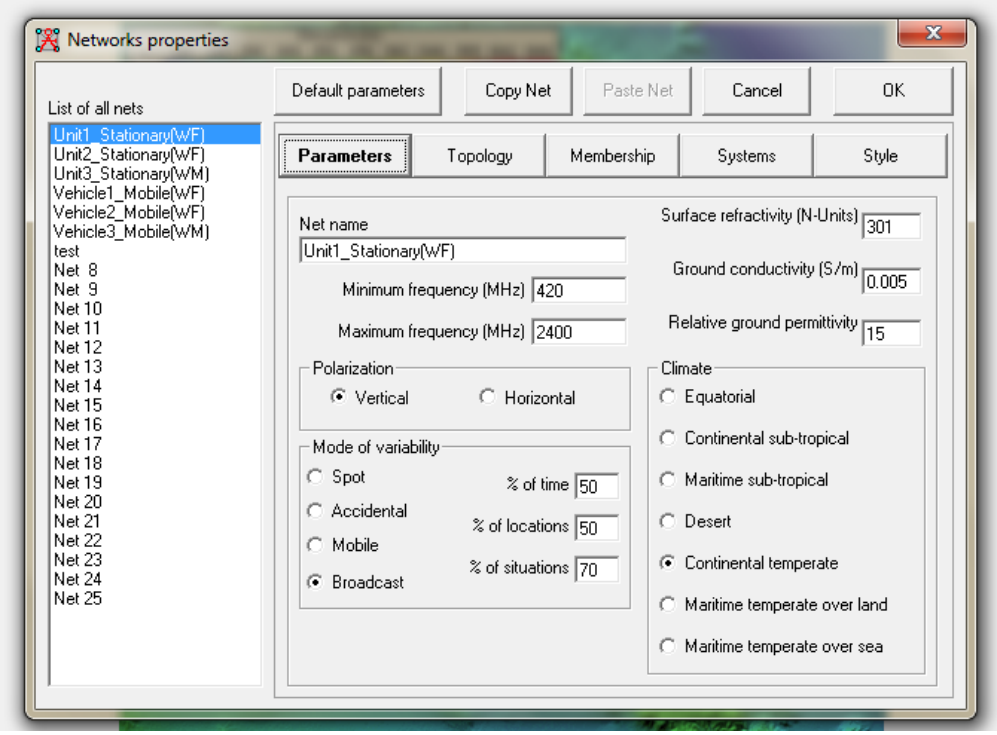

Figure 20. Network Properties Configuration Menu (from Radio Mobile)

Simulation Node Naming Convention and System Parameters						
	Node 1	Node2	Node 3	Node 4	Node 5	Node 6
Name (SPEED)	Unit1_Stationary(WF)	Unit2_Stationary(WF)	Unit3_Stationary(WM)	Unit4_Mobile(WF)	Unit5_Mobile(WF)	Unit6_Mobile(WM)
Name (Radio Mobile)	Unit1	Unit2	Unit3	Unit4	Unit5	Unit6
Primary Service	WiFi	WiFi	WiMax	WiFi	WiFi	WiMax
Frequency Range	420 MHz- 2.4 GHz	420 MHz- 2.4 GHz	420 MHz- 2.0 GHz	420 MHz- 2.4 GHz	420 MHz- 2.4 GHz	420 MHz- 2.0 GHz
Antenna Height	20 meters	20 meters	20 meters	3 meters	3 meters	3 meters
Power	20/100 Watts	20/100 Watts	20/100 Watts	20/100 Watts	20/100 Watts	20/100 Watts

Table 3. Simulation Node Naming Convention and System Parameters

To properly test the needlines functionality of EPLRS in SPEED, an EPLRS Network Plan (ENP) was necessary. Not having one, or the means of producing one, necessitated an alternate approach of simulating and analyzing nodes. Considering that EPLRS radios are set by default in the software to have a frequency of 420 MHz, frequency ranges were set to between 420 MHz and 2 GHZ for nodes labeled as WiFi. Nodes in SPEED labeled as WiMax were set to have frequency ranges between 420 MHz and 2.4 GHz. Both technologies have greater frequency ranges, but the ranges were set to encompass only the lowest frequency of each in order to make the simulations of each software suite comparable as well as that of an EPLRS radio. The corresponding nodes in Radio Mobile were set with similar frequencies and antenna heights, and were placed in the same grid coordinates. Point-to-point analyses were done for all created nodes in both software suites.

C. RESULTS

Overall, the simulation tests were insufficient to properly examine and test the use of EPLRS radio and compare handover services with WiFi and WiMax technologies. There are several aspects of each software program used and the simulation that explain the limitation.

The SPEED program was originally expected to test all aspects of the simulation including EPLRS needlines processing, homogeneous and heterogeneous service handovers, effect of terrain and elevation, etc.

SPEED is somewhat limited in its capability to conduct analysis with different types of technology media despite having the same outputs and frequency ranges. For example, the WiMax analysis tool was unable to scan connectivity to other technologies. The EPLRS analysis tools were limited to only assessing EPLRS radios and systems. Therefore, only point-to-point analyses could be conducted on all of the simulated modes. Receiver and transmitter coverage scans were also conducted but proved insufficient to support our analysis.

There were other issues in using the SPEED software. It is uncertain that land elevation was truly incorporated in all of the analyses even though Digital Terrain

Elevation Data (DTED) and Shuttle Radar Topography Mission (SRTM) was provided and properly loaded. Attempts to compensate by manually entering the elevations of each node, obtained in the Radio Mobile software, had little effect. The result of this issue led to several point-to-point analyses producing some positive results (green in color, as shown in Figure 21) despite the known elevation challenges that would be expected to degrade communications. Also, the receiver and transmitter coverage scans were overwhelmingly positive without consideration of terrain.

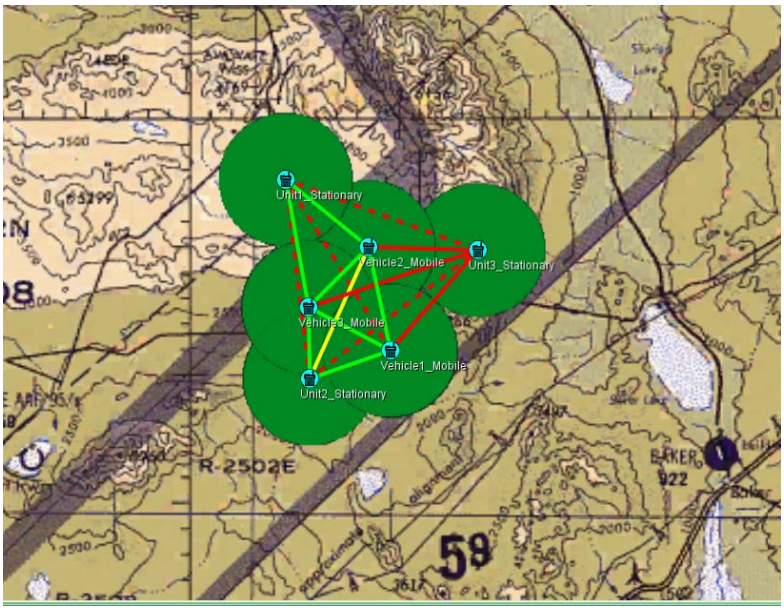

Figure 21. Example of P2P Analysis in SPEED with Receiver Coverage Analysis

The Radio Mobile program was chosen to address the shortcomings that the SPEED program exhibited as well as additional features that possibly would give more in-depth analysis within the simulated environment. The program's ability to instantly download and preserve current map and elevation data from sources like GoogleMaps was helpful compared to the procedures to get access to similar information from the NGA. The point-to-point analysis tools proved helpful in giving a comprehensive view of connectivity, effects of terrain, and anticipated receiver and transmitter ranges.

There was an incompatibility with the DTED and other map data used in each software program. Attempts were made to export and import the data used in each program in order to eliminate dissimilar analyses based on different sets of map information even though the simulated nodes were implemented with the same parameters in each program. Radio Mobile seemed to accept SRTM elevation better than SPEED, which accepted DTED information better. This perhaps contributed to the dissimilar analysis results.

Both programs were unable to conduct analysis of the interactions of the networks and users while the mobile nodes were in motion. The reasons were different for each software program. Radio Mobile does not have an inherent “on-the-move-analysis” feature. SPEED does have the feature, but it was unusable due to the lack of a networking plan. The networking plan would consist of changes in frequency, transmit power, and waypoints that chosen nodes would move along. Also, some level of encryption can be simulated in the SPEED program, though it was not considered for ease of simulation and analysis as encryption cannot be simulated in Radio Mobile. Figure 21 shows point-to-point analysis of simulated nodes with the nodes designated as mobile in different positions than the original setup with the premise of testing connectivity with simulated movement. Figure 22 shows similar analysis of identically configured nodes in the SPEED program.

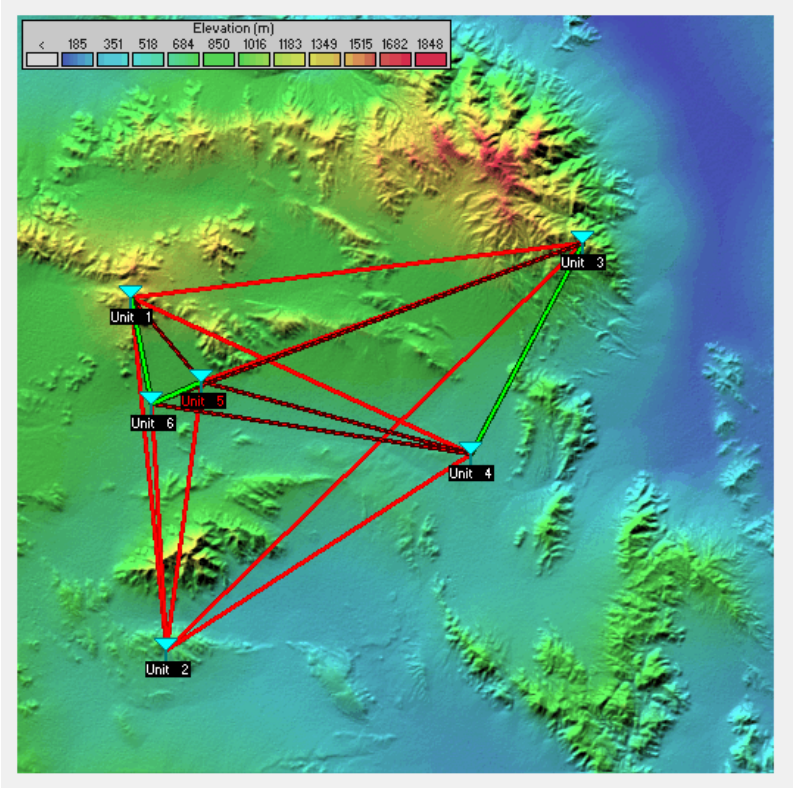

Figure 22. Nodes in Radio Mobile—Simulated Movement (100 W Power Setting)

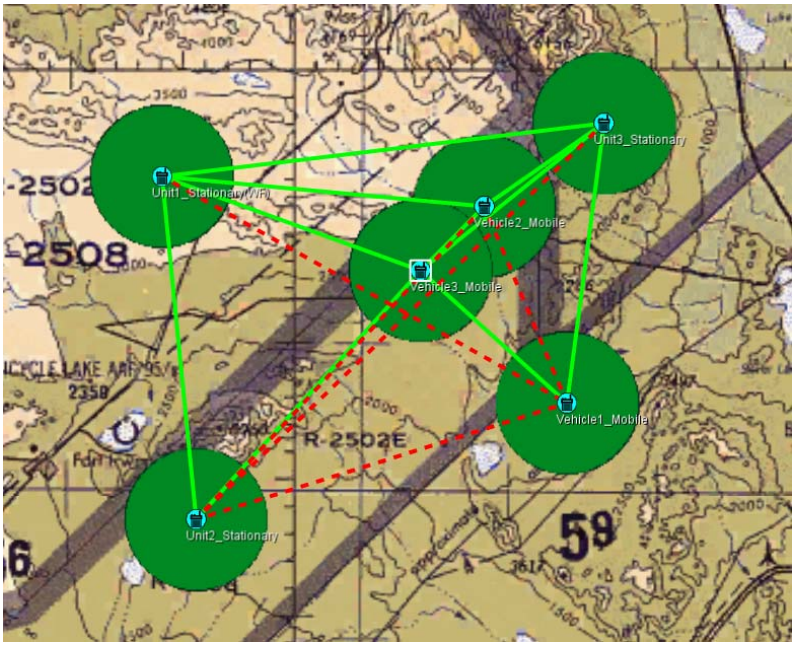

Figure 23. Nodes in SPEED—Simulated Movement (100W Power Setting)

We use Figures 22 and 23 to explain how each software program denotes network and node connectivity. Both programs utilize the same color scheme to show signal strength and connectivity status. Green denotes a solid connection while amber shows an intermittent connection; red denotes a much degraded connection or no connectivity at all. Solid lines show a clear line of sight connection while a staggered line (one color in SPEED and primary color with black in Radio Mobile) shows that terrain features (forests, hills, etc.) are affecting line-of-sight and possibly connectivity.

The green circles around nodes in SPEED, as seen in Figure 21, denote areas in which line-of-sight should be unaffected within a designated distance based on surrounding terrain features. Radio mobile provides a similar depiction, as seen in Figure 23.

Both programs were able to simulate connectivity between all nodes with some level of accuracy based on the input parameters. Initially, all simulation was to be conducted in the SPEED program. The later use of Radio Mobile gave additional insight for connectivity and point-to-point analysis, but gave different results than expected and lacked analysis tools and granularity that might have been conducive to the goals of simulating the data access technologies of particular interest. Figure 24 shows the transmitter coverage of Node 1 in relation to Node 6 based on elevation and configured settings. Whether link strength (as shown in the SPEED software) or coverage (as shown in the Radio Mobile software), green denotes ideal communication.

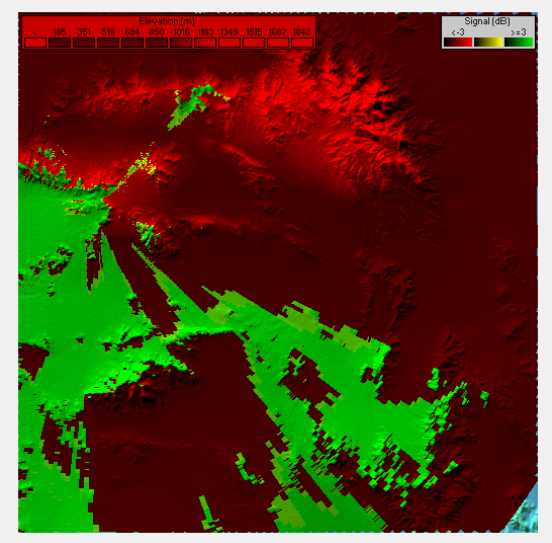

Figure 24. Transmitter Coverage Scan Results in Radio Mobile

The results of the simulations conducted added no justification to the notion that IEEE 802.21 devices and networks could benefit from using some of the characteristics of EPLRS networks. The goal of the simulations was to show nodes and networks configured with the characteristics of EPLRS networks and compare how media-independent service handover might be affected. Future research with simulations of higher fidelity should be considered in evaluating that proposed aspect of this thesis.

To ensure accuracy, we believe that a more advanced suite of software should be used that allows better simulation of data access technologies and tactical networks such as EPLRS. The Joint Communication Simulation System (JCSS) (Defense Information Systems Agency, 2015) is a recommended software suite with configurable programs and user interfaces. It is much more capable than SPEED. Built upon OPNET (Qwhatis.com, 2015), it is one of the tools that the Department of Defense uses to model, test, and validate communication systems and networks. Building custom OPNET models to be used within JCSS requires C++ coding experience as well as a solid working knowledge of the OPNET system. Other choices might include Network Simulator (ns2 or ns3) (Haddard & Gordon, 2002), both open source models; both also require significant user knowledge of the tools.

V. CONCLUSIONS AND FUTURE RESEARCH

A. CONCLUSIONS

This thesis explored how the IEEE 802.21 standard, also known as Media Independent Handover, might be used in commercial and tactical markets. Through in-depth research, analysis, and software simulation, this thesis explored two issues pertinent to implementing the standard in tactical equipment and deployments. The proposed implementations are intended to address current tactical needs while leveraging the advantages that the standard may provide in integrating multiple heterogeneous communication networks.

1. Buffer Proposal

We believe that the incorporation of additional buffers in 802.21-enabled devices and supporting network components is a feasible way to address one of the currently known issues preventing wide acceptance and usage of the standard and technology. Our research has provided deeper insight into how the protocol works and includes a case study of its application in MACE. The possibility of implementing a software-managed buffer in previous MACE initiatives was discussed with ACS personnel as it may support keeping duplicated data in preparation for a service handover for both homogeneous and heterogeneous data access services, regardless of the reason a handover is conducted. The use of additional TCP buffers working in conjunction with a master buffer in a virtual socket within the application layer of end-user devices' TCP/IP stack, as described in this thesis, requires further research, to include robust modeling via simulation, implementation, and testing. As noted, the development of an appropriate application programming interface for the virtual socket scheme would mitigate much overhead in utilization of the virtual socket concept.

Also, the issues and benefits of supporting such a modification to 802.21-enabled devices and networks were explored during the course of this thesis. Securing the data-at-rest and effects on battery charge-life were some of the consequences considered to a limited extent. The additional processing that may be necessary to duplicate some of the

data may affect battery life on some of the mobile devices. Having some of the handover and buffering functions conducted at the servers located at governing nodes may alleviate this issue. Further securing the data-at-rest could consist of utilizing encryption based on the temporary and permanent IP addresses, as seen in the configurations of the MACE project. This thesis did not address securing data-at rest nor was it intended to do so. Future research on the proposed buffer implementation would be needed to properly address it.

2. Tactical Node Placement

The stationary nature of base stations and network nodes in commercial networking environments, in which only the end-user devices move, results in more stable and predictable communications for data access technologies that include MIH scenarios than may be expected for tactical environments. Despite the stability in commercial environments, 802.21 environments still have lower levels of successful service facilitation compared to handovers within homogeneous technologies, such as WiFi to WiFi. A contributing factor is the need to associate two or more heterogeneous networks whose individual characteristics constrain compatibility.

The work presented here also explored improved approaches to addressing the use of 802.21 networks in tactical environments. Unlike commercial environments, tactical setups come with an increased level of difficulty in providing reliable service since some or all of the network components may constantly be in motion or be required to relocate at any time with minimal notice thereby causing abrupt network discontinuities.

EPLRS technology was examined and, in particular, its best attributes were studied to determine how tactical 802.21 networks may be arranged to achieve high levels of connectivity. Using two software programs, SPEED and Radio Mobile, simulations were conducted to do a comparative analysis of EPLRS networks and common data access technologies, while simultaneously trying to produce an artificial 802.21 network. Unfortunately, both programs proved to be unable to sufficiently and accurately capture the parameters of each individual technology. Furthermore, both lacked analysis tools to gauge the likelihood of successful service handovers.

The simulations were unsuitable for measuring the feasibility of using attributes of EPLRS networks to model 802.21 handover mechanisms. Thus, until further testing validates our premise, it is impossible to recommend their incorporation into future 802.21 tactical environments. Despite these shortcomings, we believe that the handovers explored here remain promising. Future research and testing are essential to substantiating the proposed concept.

B. ANSWERS TO RESEARCH QUESTIONS

This thesis evolved as the research narrowed the broad questions that were posed in the beginning. Those questions were designed to provide relevance in the context of cyber operations and the Department of Defense. This section provides short answers addressing each of them based on analysis of the research and results of the simulation as applicable.

The first two questions asked were: "What is a feasible technique, within the existing software and hardware infrastructure, to assist in seamless service handover? How might data integrity and device authenticity be maintained as the device migrates across underlying communications systems?"

The answer is that the incorporation of additional buffers in 802.21-enabled devices and supporting network components is a feasible technique to enable seamless service handover. Although we were unable to test the proposed use of additional buffers by extending a real physical device system, it is anticipated that future research and development may indeed prove it to be possible. For data integrity and device authenticity, an approach utilizing encryption based on the temporary and permanent IP addresses, as seen in the configurations of the MACE project, was suggested.

The next question was: "What type of strategic and flexible tactical deployment strategy for communication nodes utilizing the 802.21 standard will ease MIH service handovers in tactical environments compared to the stationary nodes utilized in commercial environments?"

Through software simulation and analysis, the handover concept was tested with some of the parameters and characteristics of self-healing EPLRS networks. The comparison was not sufficient for addressing some of the known issues associated with the IEEE 802.21 standard and devices utilizing it. Also, it was discovered that the software used for simulation lacked necessary capabilities therefore leading to incomplete assessments of actual EPLRS networks as well as insufficient comparisons to 802.21 service handovers. However, it is believed that a deployment strategy similar to the EPLRS network is ideal for entities that are rapidly changing in a tactical environment.

C. FUTURE WORK

1. Implementation of Buffers

The loss of data packets would be problematic if a handover occurred during the transfer of data such as large files or streaming video. The addition of buffers was proposed to mitigate or reduce the possibility of lost data packets as an 802.21-enabled device is in the course of a service handover., ACS expressed the feasibility of adding one or more buffers in the MIH protocol stack and service handover operations.

Future work to investigate the addition of buffers would possibly be extensive and might touch on multiple aspects of networking. Research and development addressing only modifications to current protocol stacks, as in the MACE initiative, would be timely and could possibly identify other complications.

2. Security and Encryption

Security and encryption are important areas of discussion and future work, both for implementation of additional buffers as well as when exploring optimum tactical deployment strategies. For the buffer implementation, ensuring that the data-at-rest is secure while in the buffer is an important concern. Threats stemming from Bluetooth attacks and poorly configured and compiled software applications and mobile operating systems may pose a threat to data-at-rest. Man-in-the-middle attacks are a threat to data duplicated or stored in secondary buffers. It is hypothesized that utilizing an encryption scheme that consists of using the Temporary and Permanent Internet Protocol addresses

(TIPs and VIPs) is only one way to assist in preventing those types of attacks. Future research should be conducted to address the multitude of issues associated with cybersecurity.

The possibility of using encryption to protect data that may be received, transmitted, or duplicated within a device is another area of future work. Whether a device encrypts all data, provides seeds for encryption keys, or acts as a randomizing agent for encryption keys, thorough research, development, and testing is imperative before implementing such encryption tools. In the case of future 802.21-enabled devices that may be developed, Federal Information Processing Standards (FIPS) compliance is vital for acceptance and widespread use within the Department of Defense.

3. Evaluation of Tactical Usage

As mentioned earlier, the simulation explored the tactical node placements of 802.21 network devices by comparing proposed 802.21 network components to components of EPLRS networks. Originally, the simulation was planned to put multiple data access network components and simulated end-user devices in notional military unit components (vehicles, operating bases, etc.) and simulate possible handover scenarios as certain components moved on a notional battlefield. Future testing of this proposal may include utilizing different software that includes the ability to test network connectivity and show changes in signal strength accurately while network components are on the move. Though modeling was conducted with the SPEED and Radio Mobile simulation software, the results were not conclusive. Further, they did not truly address the proposed technology qualities.

Other avenues of testing optimum node placement of 802.21 network components may involve the installation of ruggedized servers and antennas capable of handling media independent handover functions and other services while accounting for nodes that may move constantly and require ease of setup and teardown in order to stay adaptable to typical ever-changing tactical environments experienced by maneuver-based units.

Battlefield frequency management and frequency allocation is another aspect for future testing for tactical deployments of 802.21 elements. With the vast amount of

networking and radio equipment that units may utilize on the battlefield at one time, proper frequency management is needed to prevent data and frequency collisions as well as accidental jamming. Components may be configured to operate at preferred frequencies to separate them from other data access or radio technologies. For example, all WiFi components may need to operate at 5 MHz instead of 2.4 MHz in a particular unit. The 802.21-enabled end user devices may need to be configured to only scan for the higher range of WiFi channels in the tactical environment.

Last, the investigation of preferable service selection and commercial service restrictions is another area of future work on the tactical use of 802.21 networking. This is important so that possible issues when both tactical and commercial data access technologies are in close proximity can be avoided. High service costs incurred by units as they rely on or misuse commercial services from vendors are expected to derive the military toward the use of tactical (and mobile) wireless data access technologies. For example, WiFi is not widely used or accepted on the battlefield due to potential vulnerabilities and attacks. To mitigate some security concerns, it may be necessary that 802.21-enabled devices be configured to ignore, or even stay silent, in the presence of service providers other than those specifically intended for tactical environments.

Seeking ways to utilize the IEEE 802.21 standard in tactical environments to extend data capabilities on the battlefield was the focus of this work. Through calculated node placement and properly configured devices, it is believed to be feasible. The simulations conducted, though inaccurate, attempted to show that.

In summary, this thesis considered the IEEE 802.21 standard and sought methods to tailor previous implementations to be more conducive to tactical use with emphasis on existing technologies. If the technologies discussed are inadequate in their current forms, some of the concepts of each of those mentioned may be modified and subjected to further experimentation. As data transmission requirements are likely to increase over time, as well as the need to reduce vulnerabilities, continued experimentation with 802.21-enabled devices is warranted.

LIST OF REFERENCES

Ackerman, R. (2007, August). The Army's Network Revolution Ends. Signal Online. Retrieved November 29, 2013, from: http://www.afcea.org/content/?q=node/1359

AIR802. (n.d.). (2014, January). IEEE 802.11 Standards, Facts & Channels. Retrieved from http://www.air802.com/ieee-802.11-standards-facts-amp-channels.html

Applied Communication Sciences. (2012). MACE Phase 1 System/Software Design Description. Applied Communication Sciences.

Army Times. (2013, May 17). Pentagon Networks to Allow Official use of iPhones, iPads. Army Times. Retrieved from http://www.armytimes.com/article/20130517/NEWS04/305170026/Pentagon-networks-allow-official-use-iPhones-iPads

Boland, R. (2012, May 24). Army Turns Bases Into System Docking Stations. Signal Online. Retrieved from http://www.afcea.org/content/?q=node/2972

Bonsor, K. (2005, July 2). How the Future Force Warrior Will Work. Retrieved from http://science.howstuffworks.com/ffw.htm

Buiati, F., Saadat, I., Canas, D. R., & Villalba, L. (2011). IEEE 802.21 Information Service: Features and Implementation Issues. ICIT 2011 The 5th International Conference on Information Technology. Retrieved from http://www.zuj.edu.jo/conferences/icit11/paperlist/Papers/Information%20Security/636_Javier1.pdf

Buiati, F., Saadat, I., Canas, D. R., & Villalba, L. (2011). Overview of IEEE 802.21 Security Issues for MIH Networks. ICIT 2011 The 5th International Conference on Information Technology. Retrieved from: http://www.zuj.edu.jo/conferences/icit11/paperlist/Papers/Information%20Security/637_javier2.pdf

Cobham Defence. (2014). Cobham Defence: Defence Systems, Defence Electronics. Retrieved from http://www.cobham.com

Coxworth, B. (2011, March 26). U.S. Army Trials Tactical Smartphones. Gizmag. Retrieved from http://www.gizmag.com/us-army-looks-into-tactical-smartphones/18152/

Defense Department, Army, Fort Monmouth Historical Office. (2008). A History of Army Communications and Electronics at Fort Monmouth, New Jersey, 1917–2007. Government Printing Office.

Defense Information Systems Agency. (2015, April). Joint Communication Simulation System. Retrieved from http://www.disa.mil/Mission-Support/Enterprise-Engineering/JCSS

Defense Update. (2007, February). Integrated Digital Soldier System (IDSS). Defense Update. Retrieved January 29, 2013, from http://defense-update.com/products/i/IDSS.htm

Dutta, A., Das, S., Famolari, D., Ohba, Y., Taniuchi, K., Fajardo, V., . . . Schulzrinne, H. (n.d.). Secured Seamless Convergence Across Heterogeneous Access Networks. Telcordia Technologies; Toshiba America Research Inc., Columbia University.

Federation of American Scientists. (1998, September 12). Enhanced Position Location Reporting System (EPLRS). Retrieved from http://www.fas.org/man/dod-101/sys/land/eplrs.htm

Fielke, G. (2007). Enhanced Position Location Reporting System. Edinburgh, South Australia: Electronic Warfare and Radar Division, Defence Science and Technology Organisation.

Future Force Warrior. (n.d.) Wikipedia. Retrieved from http://en.wikipedia.org/wiki/Future_Force_Warrior

General Dynamics C4 Division. (2011). Warfighter's Information Network-Tactical: Commander's Notebook v1.6. General Dynamics C4 Division.

Global Security. (2011, July 21). Joint Network Node (JNN). Retrieved from Space: http://www.globalsecurity.org/space/systems/jnn.htm

Global Security. (2011, July 21). Mobile Subscriber Equipment (MSE). Retrieved from http://www.globalsecurity.org/military/systems/ground/mse.htm

Haddard, I., & Gordon, D. (2002, October 21). Network Simulator 2: a Simulation Tool for Linux. Linux Journal. Retrieved from http://www.linuxjournal.com/article/5929

Hanlon, M. (2007, March 25). The Dominator Integrated Infantry Combat System with Man-Packable VSAT Terminal. Gizmag. Retrieved from http://www.gizmag.com/go/7042

Hidden Node Problem. (n.d.) Wikipedia. Retrieved from http://en.wikipedia.org/wiki/Hidden_node_problem

IEEE. (2008). IEEE Standard for Local and Metropolitan Area Networks - Media Independent Handover Services. IEEE.

Information Assurance Directorate. (2012). Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package. National Security Agency.

Information Assurance Directorate. (2012). Mobility Capability Package. National Security Agency.

Jain, R. (2010). IEEE 802.21 Media Independent Handover (MIH). St. Louis, Missouri: Washington University in St. Louis.

Kapadia, V., Patel, S., & Jhaveri, R. (2010, March). Comparative Study of Hidden Node Problem and Solution Using Different Techniques and Protocols. Journal of Computing, 2(3), pp. 65–67.

Kivisto, M., & Jarvela, P. (2006). 802.16e –Mobile WiMAX. Retrieved from http://www.cs.tut.fi/kurssit/TLT-6556/Slides/3-802.16e.pdf

Mccann, S., & Ashley, A. (2014, January). Official IEEE 802.11 Working Group Project Timelines. Retrieved from http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

Oxford University Press. (n.d.). Cyber. Retrieved from http://www.oxforddictionaries.com/us/definition/american_english/cyber

Pinho, A. T. (2008, June). Implementation of the IEEE 802.21 in the Network Simulator 3. Retrieved from http://repositorio-aberto.up.pt/bitstream/10216/57942/1/Texto%20integral.pdf

Pitts, D. (2013). The Implementation of the Joint Network Node in the Global Information Grid. Naval Postgraduate School, Cyber System Operations.

Poole, I. (n.d.). UMTS / WCDMA Network Architecture. Retrieved from http://www.radio-electronics.com/info/cellulartelecomms/umts/umts-wcdma-network-architecture.php

Qureshi, R., Dadej, A., & Qiang, F. (2007). Issues in 802.21 Mobile Node Controlled Handovers. Telecommunication Networks and Applications Conference, 53–57.

Qwhatis.com. (2015). Definitions and Explanations. Retrieved from http://www.qwhatis.com/what-is-opnet/

Raytheon Company. (2014). Enhanced Position Location Reporting System (EPLRS). Retrieved from http://www.raytheon.com/capabilities/products/eplrs/

Rolta. (2012). Digital Soldier Systems: Effectual Communication Solustions for Soldiers. Retrieved from http://www.rolta.com/product1_MP_digital_soldier_system.html

Rouse, M. (2006, June). UMTS (Universal Mobile Telecommunications Service). Retrieved from http://searchmobilecomputing.techtarget.com/definition/UMTS

Smith, H. (2009). Simulation-Based Analysis and Evaluation of Tactical Multi-Hop Radio Networks. Naval Postgraduate School.

Taniuchi, K., Ohba, Y., Fajardo, V., Das, S., Tauil, M., Cheng, Y., . . . Famolari, D. (2009). IEEE 802.21: Media Independent Handover: Features, Applicability, and Realization. IEEE Standards in Communication and Networking, 112–120.

Tharp, D., & Wallace, L. (n.d.). Enhanced Position Location Reporting. Retrieved from http://www.spawar.navy.mil/sti/publications/pubs/td/3155/5a_S4papers/EPLRS.pdf

Turner, D., Carstens, C., & Torre, J. (2005 October). Future Force Warrior, Engineering Design Event Number 4. Retrieved from http://www.arl.army.mil/arlreports/2005/ARL-TR-3626.pdf

Wexler, J. (2007, February 7). Hidden nodes and Wi-Fi performance. Retrieved from Network World: http://www.networkworld.com/article/2294677/network-security/hidden-nodes-and-wi-fi-performance.html

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California